TOPEX Bytton HSDPA

Router WIFI 3G

User's Manual

2008

Company profile

TOPEX is a group of Romanian companies, founded in 1990, by ten enthusiastic engineers experienced in telecommunications. Its activity is directed to the research, development and production of telecom equipment as well as service.

Very quickly, TOPEX become the most important manufacturer of communications solutions for small to large companies as well as for telecommunications operators and providers in Romania. Our company designs equipment for all existing mobile systems (GSM/GPRS/EDGE/UMTS, CDMA/EVDO, HSDPA/TDD), including 3G technologies.

TOPEX is represented all over Romania by a wide network of local distributors through which the promotion, administration and product maintenance are running.

Due to our innovation power, authentic flexibility, real respect for our partners and the secure solutions that we provide TOPEX extended its business worldwide. Currently TOPEX delivers its products through its distributors to: Italy, Spain, France, Turkey, Netherlands, UK, Republic of Moldova, Bulgaria, Nigeria, etc.

In order to achieve effective and flawless manufacturing for its products, TOPEX has carefully organized its Research and Development Department along with its production facility. This allows TOPEX to have maximum control of all the processes involved in the complex operations related to high-technology electronic manufacturing.
Currently, 25 percent of Topex personnel are part of R&D Department and their number is increasing.

TOPEX also considered the training and the service as an integral part of the solutions it provides. Therefore, comprehensive training sessions are held at the Topex factory, complimentary for the company's clients. Service is also provided via Internet, as all Topex solutions are designed especially to allow this, at the lowest cost.

TOPEX has implemented the quality management system according ISO9001 standard certified by SRAC since 1997, respectively by IQNET since 2002. In TOPEX become a sector member of I.T.U. (International Telecommunication Union).

The main lines of products of our company are:

- Fixed-Mobile Terminals (interfaces from GSM/GPRS/EDGE/UMTS to analog, ISDN BRI and PRI, or VoIP)
- Media Gateways for TDM, VoIP, GSM and CDMA (2G,3G),
- softswitches and other Next Generation Network solutions
- Signaling Converters and Protocol Translators (SS7, SIP, H323)
- Broadband Wi-Fi Mobile Routers
- VoIP gateways (miniature, GSM/CDMA, advanced)
- ATC Voice Communication Systems (Custom systems for special applications such as (air traffic control or railway dispatching center)

For further details please visit our website at: www.topex.ro

Congratulations!

Thank you for buying the TOPEX Bytton product and congratulation for your wise choice.

BYTTON HSDPA has the following features:

- **Voice and data interface**

– simultaneous voice and high speed data transmission
– use a single mobile connection for both voice calls and data transfers, while browsing or downloading you can still make important phone calls

- **Least Cost Routing**

– by interfacing between a phone exchange and the mobile telephony network (GSM/GPRS 900/1800 or UMTS/HDSPA 2100) it cuts down the costs of fixed-to-mobile and mobile–to- fixed calls
– may be used as GSM/UMTS interface for a fixed phone or a PBX to perform routing of the calls for minimum costs, this way you will pay just the cost of a mobile-to-mobile call inside the same carrier network, instead of the cost of fixed-to-mobile call

- **Very High Throughput**

– download data rates up to 1.8 Mbps, depending upon the mobile network used*
– wireless data transfers between clients up to 54 Mbps
– wired data transfers between clients up to 100 Mbps

- **High Security**

– stateful packet inspection firewall for Internet connection
– 128 bits encryption for wireless clients, WEP and WPA with TKIP or AES encryption
– secure HTTP (HTTPS) access to configuration pages
– secure SSH remote management

- **Ease of Use**

– web based configuration interface
– embedded server for dynamic IP configuration of the clients (DHCP)

- **Advanced Internet Connection Management**

– automatic connection establishment on traffic detection
– automatic disconnection on lack of traffic
– the connection can be initiated remotely when required**
– complete network address translation (NAT) support

- **Video Surveillance Service**

– allows video monitoring using either an USB web camera or an IP camera***
– web based viewer of the video stream
– supports multiple cameras

* : this is the maximum possible rate, the actual the value depends upon network and local conditions
** :needs voice activation of the subscriber SIM used in BYTTON, from your 3G carrier
*** USB and wireless or wired IP cameras are available on demand, features varies with different models

- **Dual Flash Memory**

– for enhanced reliability, the embedded system uses a dual Flash memory
– one flash circuit is write-protected, being dedicated for the operating system (kernel)
– the other flash circuit is for the applications, which can be easily updated, upgraded or enhanced

- **Easy Firmware Updating**

– automatic update process using the web configuration interface

- **Low Power Consumption** (less than 10 Watts)

– the low power consumption means reduced heat dissipation, hence no cooling fans, no moving parts, you get higher reliability and no noise

- **USB 2.0 port**

– intended primary for web cam connection
– may be also used to connect an external modem
– current developments will allow connection of peripherals, external hard disk drives, card readers, etc. These storage devices will be shared with users from WLAN or Internet.

- **Fully Mobile Internet Access Solution**

– it is wireless on the LAN side due to embedded WiFi 802.11g/b Access Point
– also wireless on the WAN side via HSDPA connection
– the remote configuration via browser means no cables at all are required, except for power!

- **Multiple mobile networks and standards supported**

– the embedded modem multi-mode device for HSDPA/UMTS/ GPRS/EDGE/EDGE/GSM
– it is also quad-band
– this way you may use any mobile network available in your area: classic GSM (2G) in the 900/1800/1900 MHz frequency band, GPRS/EDGE/EDGE 900/1800 (2,5G), UMTS (3G) or even HSDPA (3,5G) on 2100 MHz

- **Two phone interfaces, FXO and FXS for versatility**

– the FXS interface can be used for connecting to an analog trunk of the PBX or directly to a standard phone
– the FxO interface can be used for connecting to a local extension of the PBX. This is very useful when all the trunks of the phone exchange are already used.

- **Custom voice features**

– configurable ring signal
– selectable voice /data priority
– programmable network selection

- **Advanced firewall**

– SPI firewall
– iptables for filtering and NAT

- **Static and Dynamic routing**

– You may completely define up to ten static routes, using Quagga or Kernel for routing
– Quagga routing program (RIP and OSPF protocols implemented)

- **Advanced functions for the administrator**

– may select parameters for drivers, USB connection, TCP/IP settings such as ICPM redirects

**** firmware update files are monthly published on our website

WEEE Directive Compliance

WEEE Directive

This symbol applied on your product or on its packaging means that this product fulfils the WEEE Directive. The product shall not be recycled as household waste; it will be disposed separately as sorted waste.
Regarding to WEEE Directive the recycling EE equipments must be accomplish separately in purpose of natural resources preserving and to avoid the occurring negative effects about human health and environment. The acquired product shall not be treated like household waste at the end of its life and will be returned to TOPEX Company at the address: ROMANIA, Bucharest, Feleacu Street no 10, code 014186 or given to a specialized firm.

! Please do not dispose your TOPEX product as unsorted waste (household waste), recycle it to protect the environment. Separate the packages according to waste disposal options and sort it for recycling.

For supplementary information contact us to:
Phone: +4021 408.39.00 or **www.topex.ro**

Table of Contents

1. INTRODUCTION 7
2. PACKAGE CONTENT 8
3. What is BYTTON HSDPA? 9
4. INSTALLATION 11
4.1 Establishing the best location 11
4.2 Mounting (hardware installation) 11
4.3 Identification of connectors 12
4.4. Connecting the data cables 13
4.5. Connecting the phone cables: 15
4.7. Connecting the external antennas 19
4.9. Status indicators 20
5. CONFIGURATION 21
5.1 Using the web interface 21
5.2 LAN 30
5.2.1. IP Settings 30
5.2.2. WiFi Settings 31
5.2.3. Commit 34
5.3.1. Settings 37
5.3.2. Ethernet 38
5.3.4. PPP 40
5.3.5. GRE 42
5.4 ROUTING 43
5.4.1. Firewall 43
5.4.3 Dynamic routes 50
5.5 SYSTEM 50
5.5.1. Status 51
5.5.3. Update 54
5.5.4. Password 55
5.5.5. Defaults 56
5.5.7. Load 57
5.6 SERVICES 58
5.6.1 DDNS 58
5.6.2 NTP 59
5.6.3 Webcam 60
5.6.5 PWC compatible cameras 60
5.6.5. Reset 61
5.7 SIM 62
5.7.1. SIM Status 62
5.7.2. SIM Settings 63
5.8. VOICE 65
5.8.1. Phone Connections for BYTTON HSDPA 65
5.8.2. VOICE Status 67
5.8.3. VOICE Settings 68
5.9 Optimizing WiFi Performances 70
5.9.1. Network physical configuration 70
5.10 Status Page 71
5.12.1 LAN 73
5.12.3 System 74
6. TECHNICAL SPECIFICATIONS 77
7. OPERATING ENVIRONMENT 79
8. APPLICATIONS 80
9. Glossary 83

Revision E, edition march 2008.

1. INTRODUCTION

Embedded Modem

The embedded modem of BYTTON is a HSDPA/UMTS/GPRS/EDGE/GSM multi-mode device. It measures in real-time the RF signal level strength of the mobile network and lets the user to freely choose the 2G/3G network. Thus it provides access rates up to the maximum possible for each network.

This way you may talk, download files or surf the Web without cabled connections almost anywhere, at any time. When you are out of the coverage of high speed networks such as HSDPA/UMTS, you can still get services on the wireless Internet with alternative access via GPRS/EDGE/GSM network in your area. The embedded multiband modem covers almost all of the frequency bands of the world!

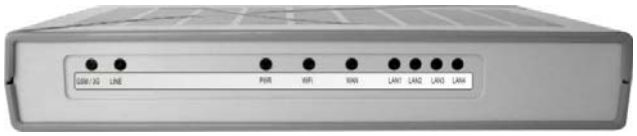
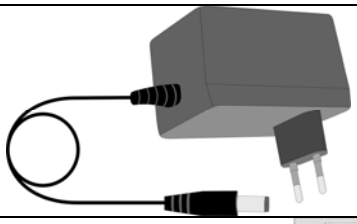
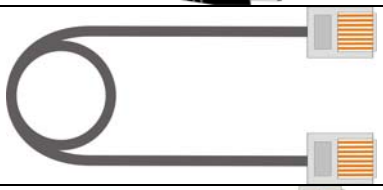
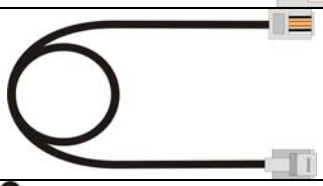
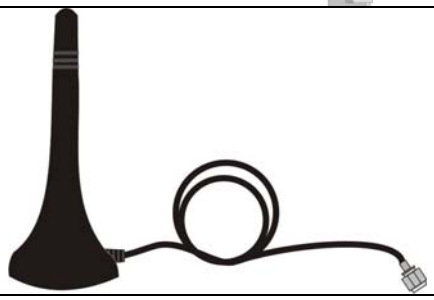
WiFi

Wireless LANs are complementary extensions to existing wired LANs, offering complete mobility while maintaining continuous network connectivity to both corporate and home Intranets. PC users stay connected to the network anywhere throughout a building without being bound by Ethernet cables or other LAN wires. This is accomplished through the use of Access Point functionality of BYTTON HSDPA. The TOPEX equipment with built-in Internet gateway capability allows your house or company to share an UMTS account or other broadband connection, working simultaneously from different rooms, without need for cables or wires. The embedded Access Point of the TOPEX Gateway complies with wireless standards IEEE 802.11g and 802.11b. The 802.11g is as extension to 802.11b (used in majority of wireless LANs today) that broadens 802.11b's data rates to 54 Mbps within the 2.4 GHz frequency band using OFDM (orthogonal frequency division multiplexing) technology.

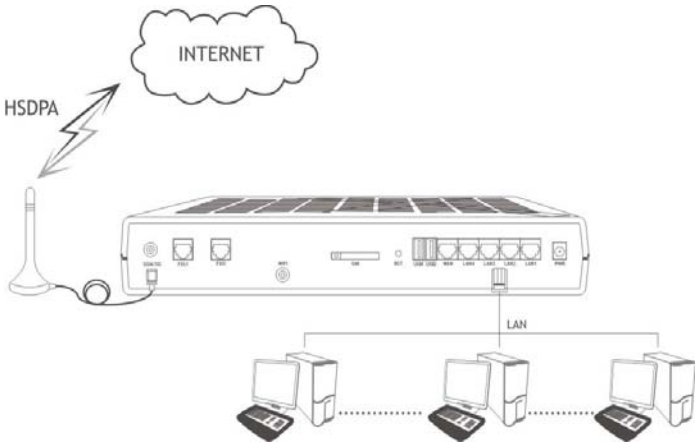
In order to ensure a correct installation / configuration and a good operation of the BYTTON HSDPA equipment, the manufacturer strongly recommends you to study this manual before attempting operation.

2. PACKAGE CONTENT

The component elements that you may identify upon opening the BYTTON HSDPA package are shown below. When you open the equipment package, please ensure, using this list of items, that you have the full content.

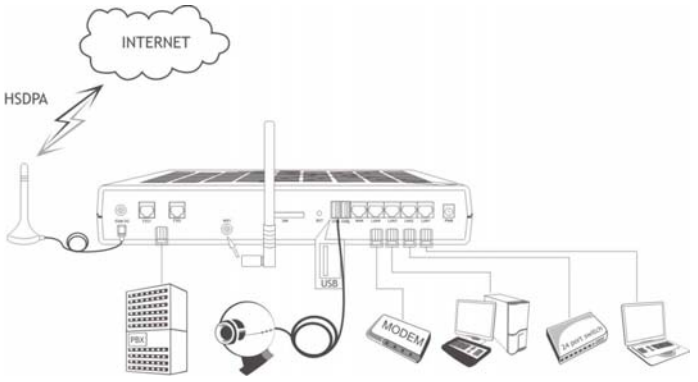
Component Image	Component Description
	BYTTON HSDPA unit in its plastic case. It is a router and firewall for a wired and/or wireless local computer network, which allows secure, mobile, high-speed access to Internet using the 3G network
	Power supply: mains adapter Input: 100-240V $_{A.C}$ Output: 12V$_{D.C}$. / 2A Max. Power: 25 W
	Ethernet cable for local network connection A piece of UTP straight cable, with RJ-45 connectors.
	Cable for PBX Flat phone cable with RJ-11 connectors
	Antenna for HDSPA Multiband, with magnetic base and 2,5 m long cable
	Stick antenna for WiFi
-	CD with User's Manual
-	Quick Install
-	Warranty Certificate

3. What is BYTTON HSDPA?



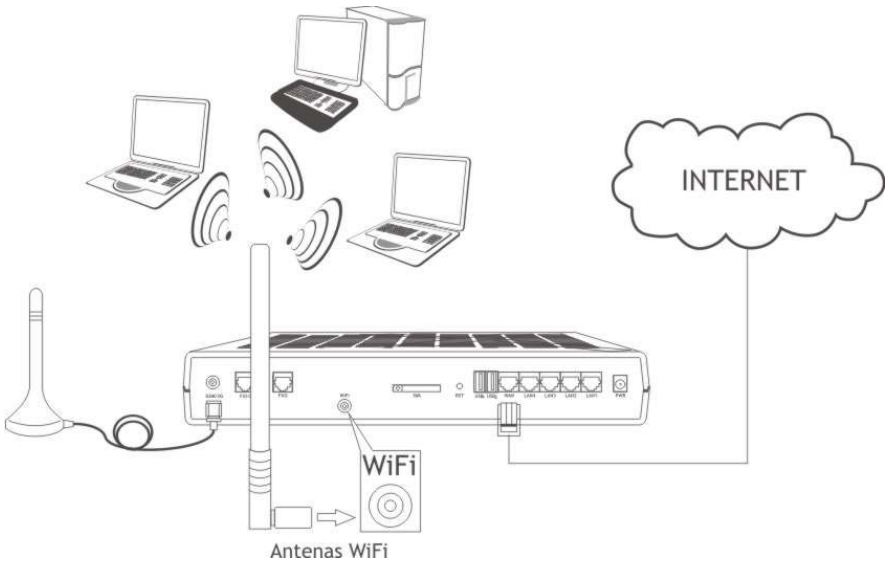
Still, if you are in an area where you have only UMTS or GPRS or even GSM coverage, you may use BYTTON in conjunction with the respective networks.

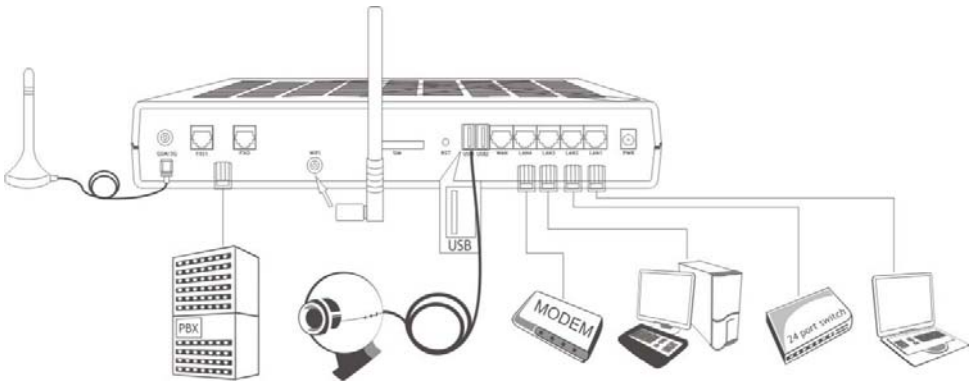
The BYTTON HSDPA equipment is versatile advanced router for wireless broadband Internet access using 3G technology.
At the same time, it is a voice and data interface between a single phone or a PBX exchange and GSM/GPRS/EDGE/HSDPA mobile network.
As **data router**, BYTTON achieves a direct connection, transparent for the user, between the local network (Ethernet and/or WiFi) and the HSDPA/GSM/GPRS/EDGE/UMTS mobile communications network.
For wireless WAN connection, it uses an embedded radio modem for the HSDPA mobile network. Its 3G capabilities assure high speed Internet access.



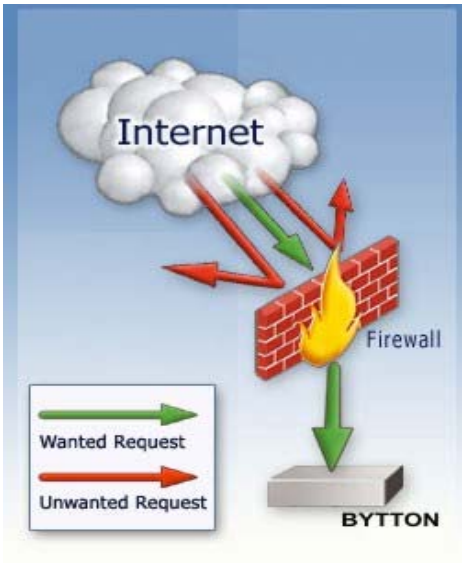
The parameters of the FXO and FXS interfaces are software programmable, by means of the web interface. This facility is very helpful when your phone exchange has only ISDN interfaces or there are no available analog trunks (all of them are used).

As a **voice interface**, it allows wireless connection of the local subscribers and decreases the cost of fixed–to-mobile and mobile–to-fixed calls. BYTTON achieves a direct contact between a trunk or a local subscriber extension of a PBX over the mobile network. This way the fixed-to-mobile calls are converted into mobile-to-mobile calls. Thus you will pay only the mobile-to-mobile cost.
Since BYTTON HSDPA features both FXO and FXS interfaces, it is highly versatile: you may connect it either to a trunk of the phone exchange or to a local extension of the same phone exchange.





All computers on the wired or wireless local network can access the Internet through the Topex HSDPA Router, using only a single external IP address.



One can rest assured that the local area network connected to our product is safe because we have implemented a very powerful firewall and intrusion detection system.

The Topex BYTTON HSDPA Router makes usage of NAT (Network Address Translation) and SPI firewall to ensure protection for your local network, wired or wireless.
The features of the firewall are identical to those available to Linux servers throughout the world, which are well renowned for their safety.
This firewall is fully configurable, but it is also easy to use for beginning users.

Because our product is Linux based, applications to enhance BYTTON HSDPA or to customize it can be quickly designed by our software developers, according to the special needs of various clients.
Our best technical experts are available for your technical questions around the clock, if you sign up our technical support offer. In addition, the software upgrades can be done remotely via Internet, and are free of charge.
BYTTON HSDPA is a highly versatile solution; its embedded firmware can be easily upgraded over the Internet.

4. INSTALLATION

In order to ensure the proper operation of the BYTTON HSDPA equipment you must follow the set-up steps shown below:

- Establish the best location
- Mounting (Hardware installation)
- Identification of connectors
- Connecting the data cables
- Connecting the phone cables
- Configuring and installing the SIM card
- Connecting the external antennas for HSDPA and WiFi
- Setting the PIN or PUK code, if required
- Power up

4.1 Establishing the best location

In order to determine the best location for the TOPEX router please have in mind these considerations:

• If you use wired connections, the length of the Ethernet cables that connects the Bytton routers the network must not exceed 100 meters.

• BYTTON HSDPA should be placed on a flat, sturdy surface located as far from the ground as possible. A high location, on the wall or on top of a desk or a shelf is best both for the HSDPA connection and for the Access Point. Also, BYTTON should be kept clear of obstructions and away from heat sources, direct sunlight and heavy-duty electrical equipment.

• To ensure good coverage to all of the wireless mobile devices in your area BYTTON HSDPA should be installed in a central place in the building. Normally the antennas should be in vertical position, but if reflections occur, you may get better results by changing their orientation.

• For power supply, use only the adapter shipped with BYTTON. The jacks of different power supplies may fit but the polarity, current, voltage or regulation factor may not be compatible.

• While the device is in operation, the antennas of the BYTTON HSDPA unit should be at least 30 centimeters away from any human being.

4.2 Mounting (hardware installation)

The Topex BYTTON HSDPA router may be mounted either horizontally, by means simply placing it on a flat surface, or vertically on a wall (using the mounting kit).

Horizontal mounting
The surface must be level and strong enough to hold the weight of BYTTON HSDPA together with its cables (power supply, wired LAN connections, telephone, USB etc). A desk, table or shelf is good place for the installation of BYTTON. . In this case, the WiFi antenna should be in vertical position (at right angle to the box of the equipment)

Wall mounting
The equipment may also be mounted on a wall, by means of the kit included in the package.
It is recommended you use a pattern to secure the device to the wall. Also, you should use professional installation to reduce the risk of injury and damage. In this case also the WiFi antenna must be in upright vertical position, but it will be parallel to the equipment's box.

For mounting BYTTON HSDPA on a wall you should use the mounting kit (plastic dowels, woodscrews, etc) provided by Topex.

On the back there are two pairs of mounting holes, 160 mm apart. The two pairs are located 100 mm one from another, allowing you to fasten BYTTON to the wall either connectors up or indicators up.

Perform the following steps:

- mark on the wall the position of a pair of holes, spaced at 160 mm apart
- drill the holes in the wall
- forcibly insert into the holes the plastic dowels
- thread the metallic woodscrews into the plastic dowels leaving the end to protrude outside for some 5 mm
- hang the case of BYTTON HSDPA in the two metallic woodscrews and push it down a little to get it fixed
- if it does not lock properly, you should adjust the screws

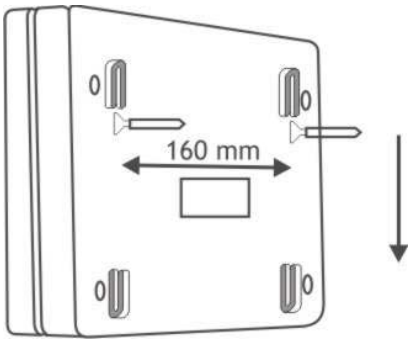


Figure 1. Mounting BYTTON HSDPA on a wall

No matter if it is installed horizontally or vertically, the best location for BYTTON HSDPA is in the middle of the place where you want to have wireless coverage. Installing BYTTON on a shelf higher up, with no obstructions around, ensures the best performance, both for WiFi and for the HSDPA modem.

Take care to ensure adequate cooling of the Bytton terminal.

4.3 Identification of connectors

Topex BYTTON HSDPA features several external connectors, as described below.
On the back panel of the equipment there are, from left to right:

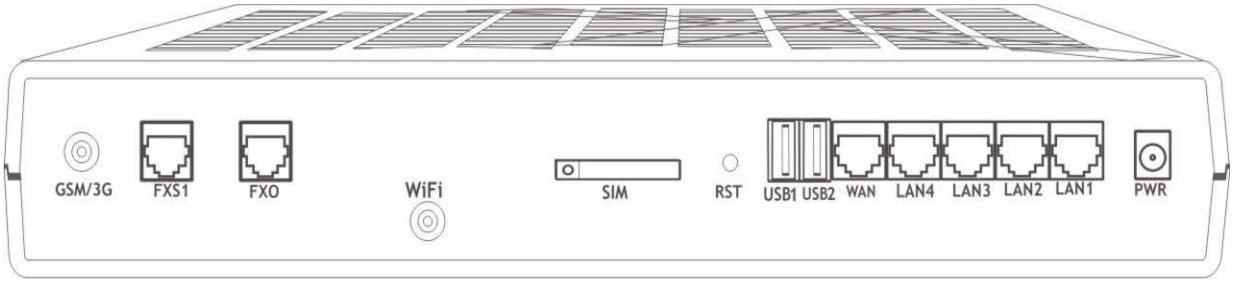


Figure 2: Connectors of BYTTON HSDPA

- a circular RF connector (female), for the HSDPA antenna **(labeled GSM/3G)**
- a RJ-11 connector for the FXS telephone interface **(labeled FXS1)**
- another RJ-11 connector for the FXO telephone interface **(labeled FXO)**
- the slot for the SIM card (**labeled SIM**)
- in the middle, a little below the centerline, a second RF connector (male) for the antenna of the 802.11 b/g wireless access point **(labeled WiFi)**
- the black Reset button, recessed (**labeled RST**)
- the USB-A slot (**labeled USB**)
- A RJ45 connector for the external network (**labeled WAN)**
- four female RJ45 connectors for the local network connections, **(labeled LAN4 to LAN1)**; the four LAN connectors are numbered in reverse order, as to correspond to the LAN indicators on the opposite side, which are direct order.
- The right, the round connector for the power supply jack, (labeled **PWR)** ($12V_{DC}$)

4.4. Connecting the data cables

To ensure a proper functioning of the BYTTON HSDPA unit, you must make the right cable connections, as described below.

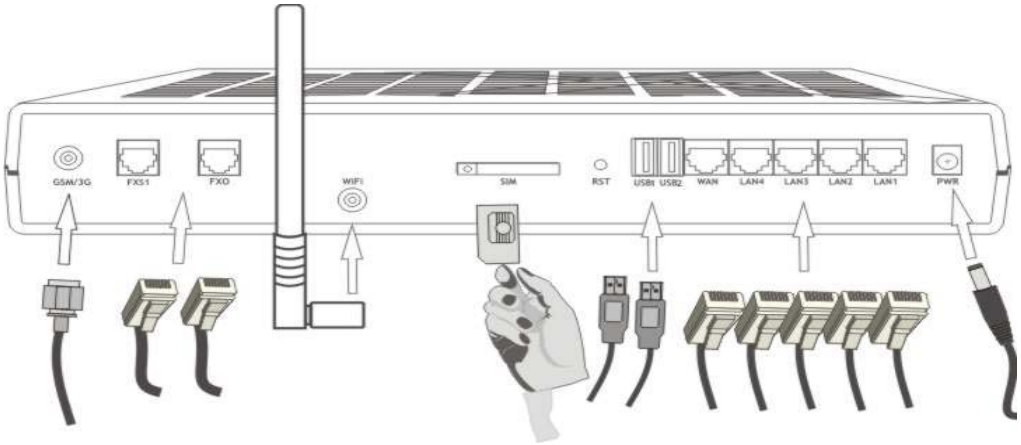
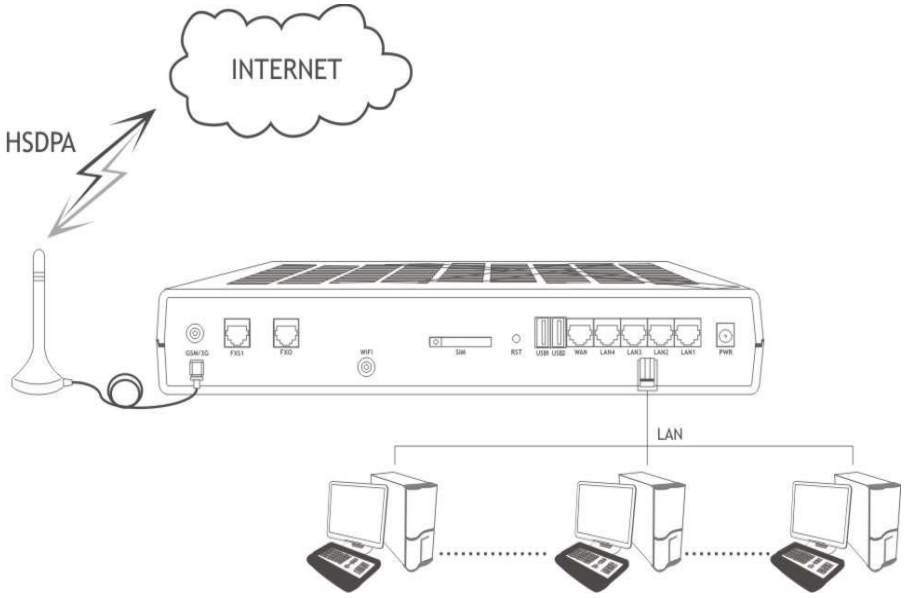


Figure 3: Connecting the cables

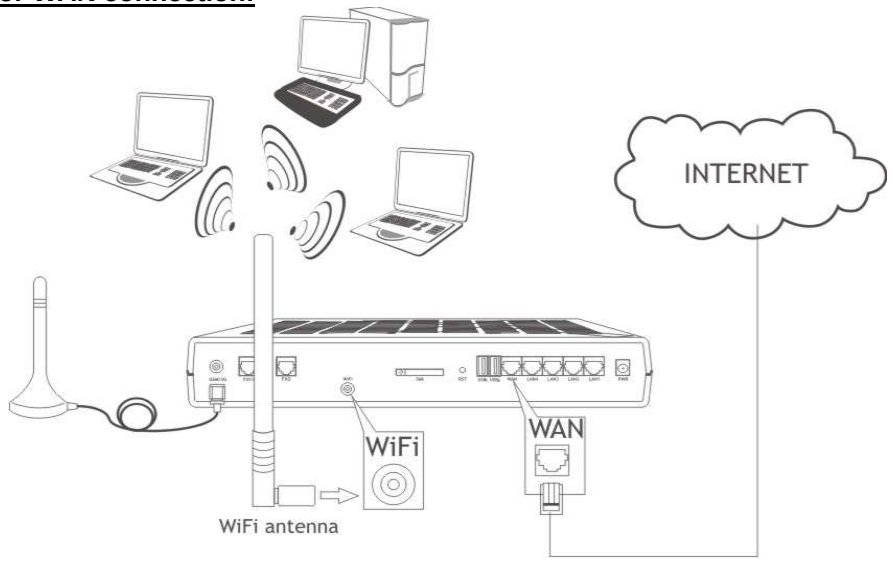
For local network connection:

Use standard UTP network cables (CUT 5) fitted with RJ45 connectors at both ends. The cables can be either straight-through or crossover, since the switch of BYTTON HSDPA is auto-crossover. One short length of RJ-45 cable is supplied with the TOPEX BYTTON Router. You may use either 10Base-T or 100Base-T connection, and both types of Ethernet connections maybe used on the same time.



The network cables are to be inserted with one end into the RJ-45 sockets of the BYTTON HSDPA equipment labeled **LAN1** to **LAN4**. The opposite end of the UTP cable can be inserted directly into PCs or in switches or hubs. The corresponding LED indicators of the front panel should light up, showing physical connection and data traffic on the respective Ethernet interface.

For WAN connection:



Plug one end of the cable into the RJ45 port labeled "WAN" on the rear of the TOPEX BYTTON HSDPA and the other end into the Ethernet port of the ADSL or Cable modem.

For Wireless connection:

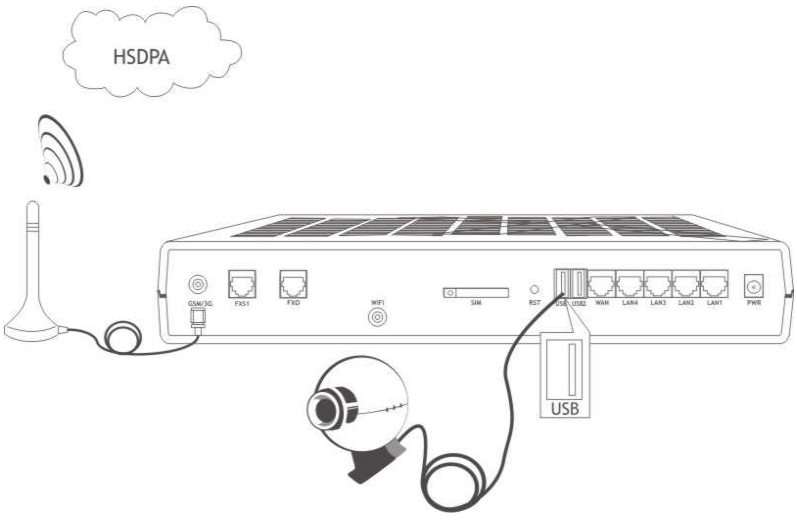
When a wireless device enters in the coverage area of BYTTON, it will be automatically connected. For settings, refer to the User manual of your wireless adapter for associating with the BYTTON HSDPA router. The default SSID of the TOPEX router is "ByttonHSDPA", encryption is disabled and open system authentication is used. You can modify these default settings as you wish.

For USB connection:

Plug the USB cable of the device into one of the USB slots of the BYTTON HDSPA equipment.

Currently it supports USB webcams that are compatible with PWC Linux drivers. For details see http://www.saillard.org/linux/pwc/.

Development in progress will allow also connection of various USB devices or peripherals, such as printers, scanners, HDD or Flash card readers for extended storage.



If you need to connect several USB devices to Bytton, you should use an USB hub to "multiply" the single USB slot of the Bytton equipment.

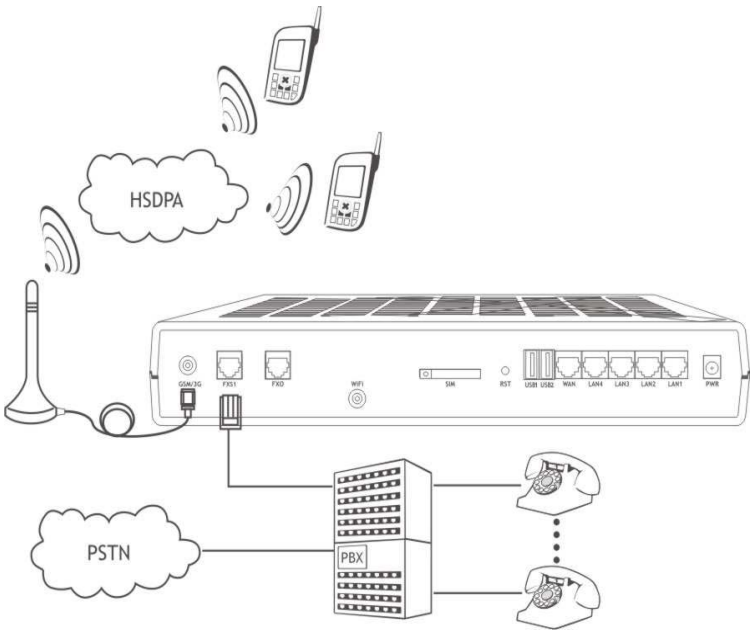
4.5. Connecting the phone cables:

You may use one of the phone interfaces, **either** FXS **or** FXO. For connection, BYTTON HSDPA is shipped with a flat telephone cable, wired on both side with male RJ11 connectors.

Connecting the telephone cable for FxS interface

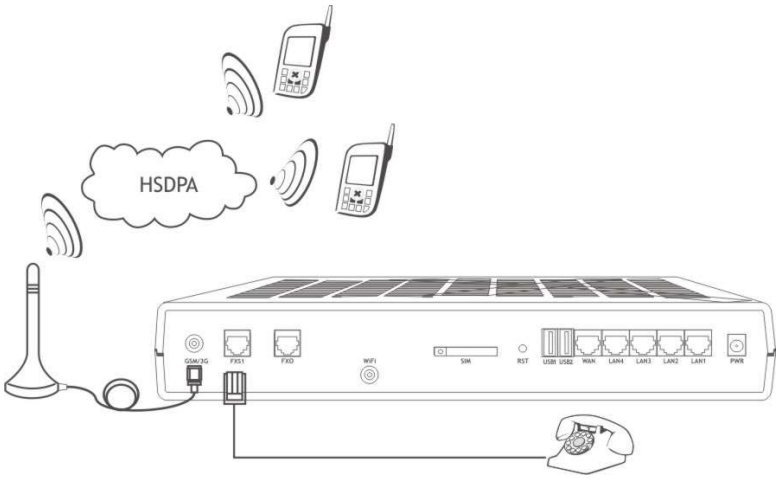
Connect the telephone cable with one of the end to the FXS connector of BYTTON and the other end to an **analog trunk** of PBX.

Should the phone exchange have terminal trunks not equipped with RJ-11 connectors, you must connect the two middle wires of telephone cable directly to internal connector of the PBX exchange.



Alternately, you may connect the telephone cable with one of the end to the FXS interface of BYTTON HSDPA and the opposite end directly to a standard (fixed) phone.

In this case you won't have the routing facilities of the phone exchange, but you still be able to make voice calls while transferring files or browsing the Internet.



Note: BYTTON HSDPA features analog phone interfaces, so it must not be connected to an ISDN interface (digital trunk) of PBX exchange. For connection to an ISDN exchange you should use wireless equipment specially designed for ISDN phones. Improper installation of BYTTON HSDPA equipment might lead to damage of BYTTON or PBX. (If you join a local subscriber line of PBX exchange to the FXS connector of BYTTON then both equipment will generate current into the connection cable, so the Bytton router and PBX the exchange could be damaged).

Connecting the telephone cable for FXO interface

If you use the FXO interface of BYTTON HSDPA, connect the phone cable with one of the end to the FxO connector of the equipment, and the other end to a **line interface** (local extension) of your PBX.
Take care NOT to connect the FXO interface to a trunk (outgoing line) of the PBX.
Also, the FXO interface of BYTTON must be properly configured (use the Web interface to change the settings).

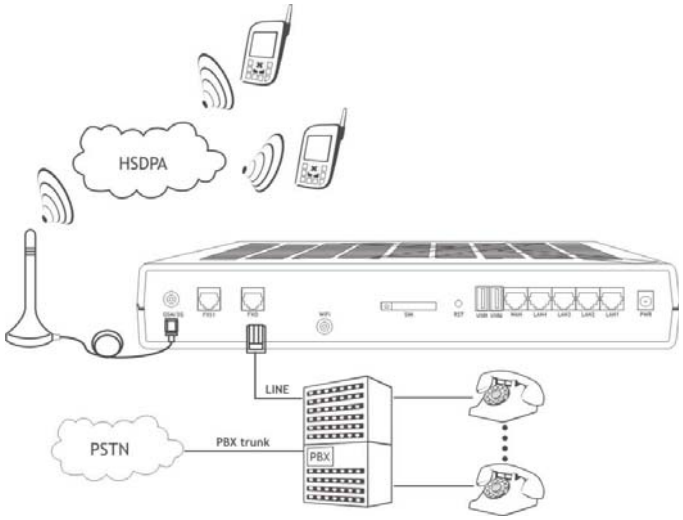


Figure 4: Connecting the telephone cable for FXO interface

Note: In this case, if no restrictions exist for subscriber access rights assigned for extension where BYTTON HSDPA was installed, any caller from fixed network who rings to the BYTTON number can obtain the access to outgoing trunks. So his calls will be billed to the owner of the PBX.

For avoiding this you have the following solutions.
- either configure the phone exchange to reject the outgoing calls on the extension where BYTTON HSDPA interface is connected
- or set the BYTTON HSDPA equipment so that when it receives a call from mobile network, it will automatically direct the call to a specified extension (generally the operator's desk).

For power supply:

To power the BYTTON unit, just insert the jack of the power supply adapter into the supply connector. Do **not** yet plug the adapter into the $230V_{A.C.}$ mains outlet on the wall. The special adapter from Topex, which is part of the Bytton HSDPA package, supplies the voltage required to power the equipment. It is an external power supply adapter.

Note: *The adapter is the disconnection device (there is no POWER switch), so the 230 V_{AC} socket-outlet shall be installed near the equipment and shall be easily accessible.*

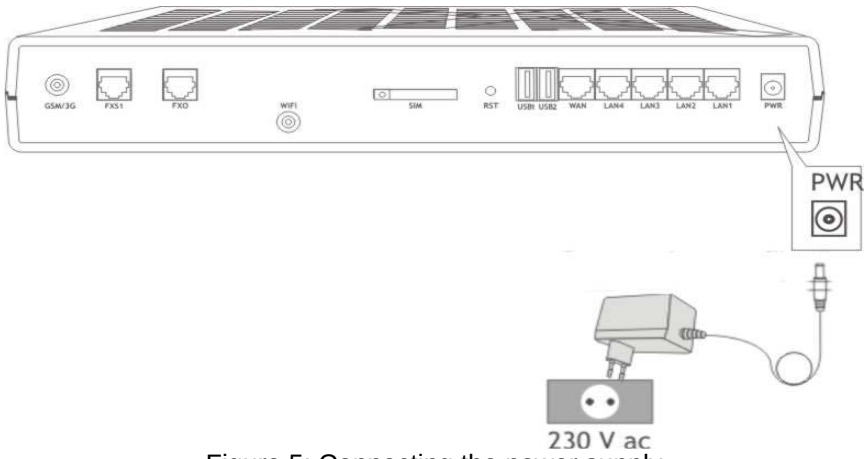


Figure 5: Connecting the power supply

Warning !
- Use only the power supply adapter shipped in the equipment package. Using of other kinds of power supplies may cause damage to the equipment.
- To avoid accidents or damage to the equipment, follow the steps described earlier. First, connect the antennas, and then the power supply adapter.
- You should avoid connecting or removing the antennas while the BYTTON HSDPA equipment is powered.

4.6. Configuring and installing the SIM card

In order for the BYTTON HSDPA router to work, it must have a valid SIM card with subscription to the GSM/GPRS/EDGE/UMTS/HSDPA operator where you want to connect to.

Configuring the SIM card

The SIM card that is used must be active.

- The SIM card must be configured **before** it is inserted into the slot of BYTTON HSDPA.
- For configuring the SIM card you may use an **ordinary GSM cellphone**.

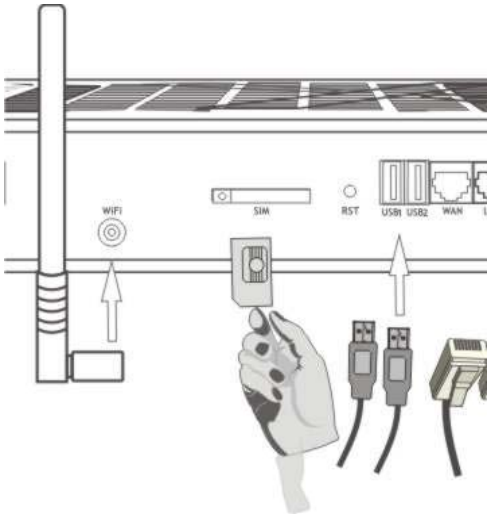
The required configurations are:

⏩ *PIN CODE REQUEST* – if you disable (from the menu of the mobile phone) *PIN CODE REQUEST* security option, then you will not be asked to enter it. Alternatively, the PIN code can be enabled and you may enter it form the Web page used for configuration. *In this case, take care to enter the correct PIN code **before** inserting the SIM card, to avoid PUK locking!*

⏩ *Disable GSM services* – GSM operators offers you different supplementary services for calls. When you use the BYTTON HSDPA interface is recommended that these options to be disable, because they are available only with additional costs.

Inserting the SIM card

The SIM card must be inserted into the special slot of the TOPEX BYTTON equipment.



The slot for SIM cards is located on the rear panel (the one with the connectors), in the middle, as shown in the next image.

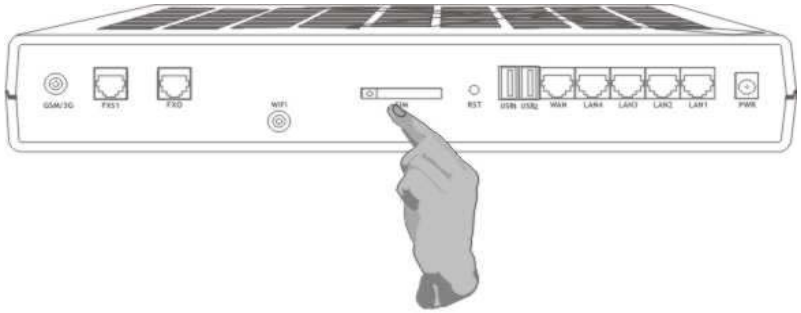
For inserting or extracting the SIM card use the mobile holder (removable tray) for the SIM card.

Use the little yellow button to activate the holder.

Handle with care when inserting or extracting SIM card.

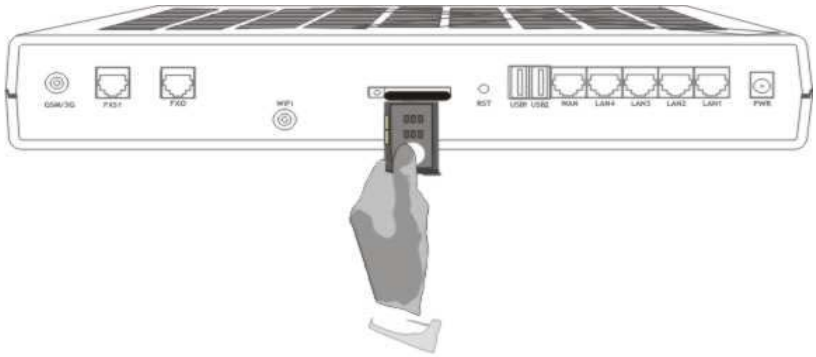
! When inserting or changing the SIM card, the equipment must be powered off.

For inserting the SIM card follow the next steps:



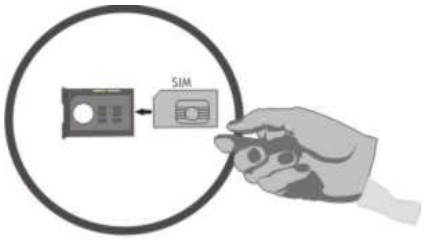
STEP 1

1. Push the little yellow button to eject the SIM carrier.



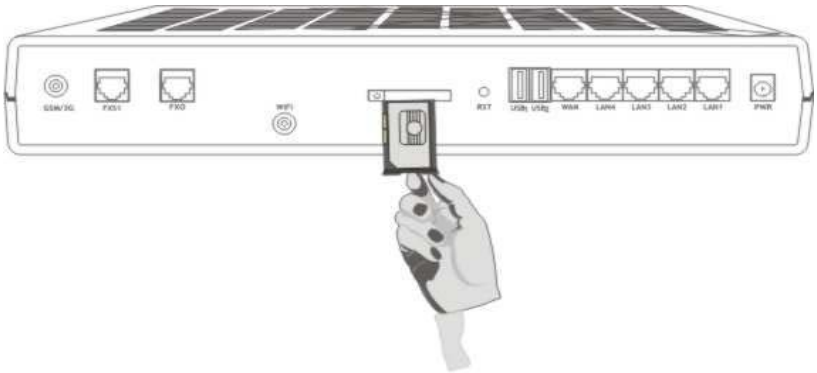
STEP 2

2. Pull out the holder (tray) for the SIM card.



STEP 3

3. Insert the SIM card into the holder, with the cut (notched) corner orientated upwards and the side with contacts toward you



STEP 4

4. Insert the holder with the SIM card back into the slot and push to close. Be careful not to drop the SIM out of the tray and to insert the holder properly into the slot!

4.7. Connecting the external antennas

To ensure a good quality of transmission and reduce radio interference use the antennas shipped in the BYTTON package. These antennas are for the respective frequency bands (multiband for GSM/GPRS/EDGE/UMTS/HSDPA network and 2,4 GHz for WiFi).
The antennas must be connected to BYTTON HSDPA via the respective RF circular connectors on the back panel of the case. The cable for HSDPA antenna must be threaded into the circular connector of BYTTON HSDPA labeled "GSM/3G", while the stick antenna for WiFi into the other RF connector (to the right) as shown in the following drawing.
Note that the connector for the Mobile network is female, while the one for WiFi is male (with protruding pin) so there is no risk of inserting the incorrect antenna.

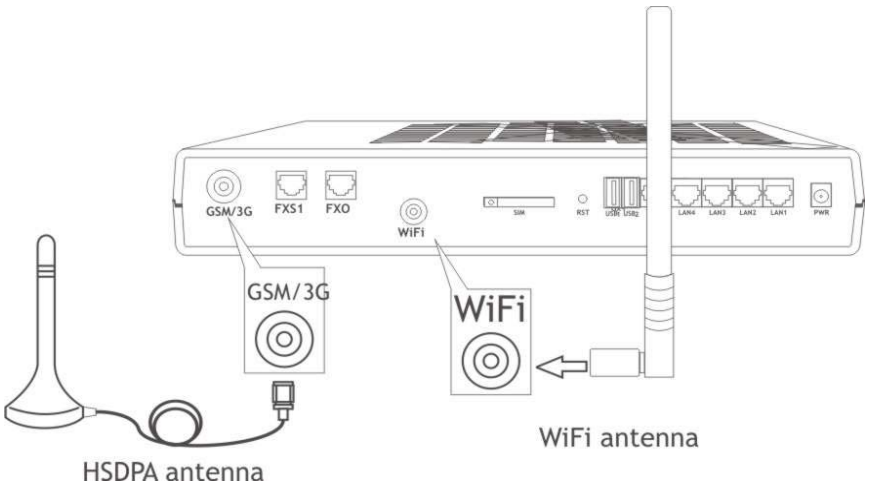


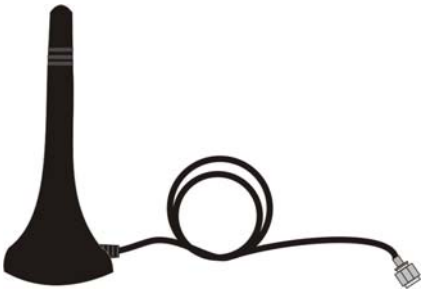
Figure 6: Antenna attachment

If your site has low level of 3G signal, it may not be possible to use the full HSDPA technology without a special, high gain antenna. You should get such an antenna and install it in a higher position (the roof of the building), directed towards the base station of the mobile network carrier, in order to get best results.

Warning! *Don't use excessive force. Make sure the antennas are securely screwed into the RF connectors, but do NOT use a spanner or screw key, which could damage the antenna connectors! Tighten the flange lightly, by hand.*

The antennas have vertical polarization, they should be placed in vertical or horizontal position, depending of the local field condition.

! You should fasten the antenna on a safe (with great stability) and flat area, even one that is not magnetic.



The following table shows the main characteristics of the multi-band stick antennas with magnetic base (currently supplied with the BYTTON HSDPA package).

Frequency bands	GSM 890-960 MHz PCN 1710-1880 MHz PCS 1850-1990 MHz UMTS/HDSPA 1920-2170 MHz
Gain	2 dBi
Polarization	Vertical
Height	Total 73 mm Active stick 43 mm
Base	Magnetic, diameter 2,8cm
Cable	Type RG174, length 2,5 m
End Connector	Nipple, male

Notice:

- The BYTTON HSDPA unit and its antennas should be placed such as to be as far as possible from appliances or office equipment that is sensitive to radio interference (microwave ovens, copiers, TV sets, PC displays, and multimedia systems). For best results, try to find for the HSDPA antenna a place of maximum signal reception.
- In addition, the antenna must NOT be located near heavy-duty equipment that may generate electromagnetic interferences, such as electric motors or heaters.

4.8. Power up

Power up BYTTON HSDPA by inserting the adapter into the wall outlet. The Topex router will start working. You should see the PWR indicator LED lighting up.

4.9. Status indicators

BYTTON HSDPA several optical indicator (green or bicolor LED) that shows the status of the device. This indicator light up continuously or flash to show data traffic. In normal operation the LAN, WAN, WiFi or respectively NET indicators must be blinking. The LINE indicator shows the active status of the phone line.

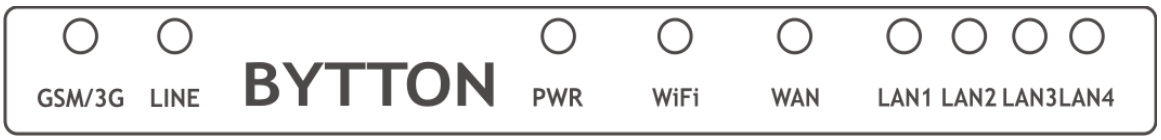


Figure 7: LEDs location

GSM / 3G – Green LED. Off indicates no mobile network connection, On = data connection active.

LINE – Red LED. Lights up to show the phone interface is in use. When it is ON, it indicates the phone line (FXS) or the junction (FXO) is engaged.

PWR – Green LED. Off = no power, On indicates that BYTTON HSDPA is powered. . Of course, if the power supply voltage is off, no indicator LED will light!

WiFi – Green LED. Off = not in operation, On = wireless system ready, blinking indicates activity of the embedded 802.11 b/g Access Point

WAN – Green LED. Indicator for the WAN Ethernet connection. Off = no cable connected, On = physical connection to Ethernet network (an UTP cable was connected to the respective input), flashing = shows data traffic (send or receive) through that connector

LAN 1 … 4 – Green LED. Off = no cable connected, On = physical connection to Ethernet network (an UTP cable was connected to the respective input), blinking = shows data traffic (send or receive) through that connector. Note that the four LAN indicators are numbered in direct order, as to correspond to the LAN connectors on the opposite side.

5. CONFIGURATION

BYTTON HSDPA can properly perform its functions of wireless high-speed router with the default settings. However, it can be easily configured to meet various usage scenarios. "Configuring" or programming the equipment means adequate setting of all the parameters. The embedded Linux firmware allows you to configure BYTTON HSDPA without the need of additional software on the computer used for programming. You just need a web browser as configuration terminal. This means that BYTTON HSDPA may be used on **any computer platform** and is not restricted to a certain operating system!

Using the web browser, the configuration can be performed remotely: the desktop PC or notebook may be connected to the TOPEX Router either directly or through a hub and the connection can be wired (Ethernet) or wireless (WiFi). In this last case, no cables at all are required to program BYTTON HSDPA, except for power!

For this wireless connection your PC or notebook must have an IEEE 802.11g/b compatible device installed. This can be an Ethernet adapter, a PCMCIA card, an USB device, etc. Recent notebooks already come with embedded the 802.11g/b capability. You should also disable WEP (encryption) and set the SSID for your wireless LAN device to "default" or to the name used by BYTTON.

Prior to using this HDSPA Gateway you should check the basic settings to guarantee it will work in your environment (for instance, it may be required to change the default IP address). When the IP Plug and play feature of Bytton is, you don't need to bother with TCP/IP settings enabled, you may connect directly to configure the BYTTON HSDPA equipment or to access the Internet through the wireless network.

5.1 Using the web interface

The default address of the webpage of Topex BYTTON device is 192.168.1.1.
It is recommended that you use this address, if the configuration of your local network allows this.

Set up a connection

First, you should establish an Ethernet connection to the Bytton HSDPA unit you want to configure.

Go to "Network Connections" on your computer and define a connection to be used for the Bytton HSDPA router.

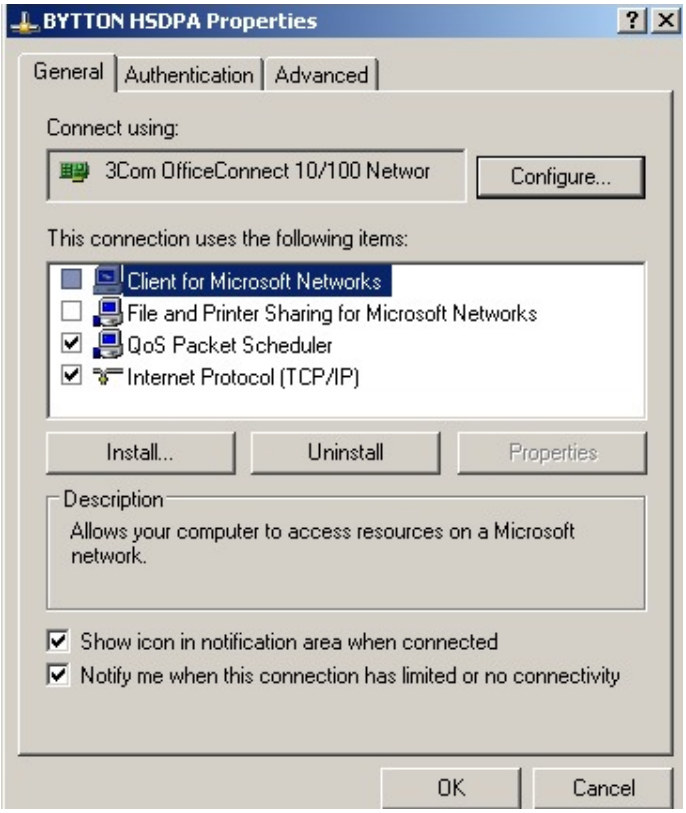
You should use for it a significant name, such as "Bytton HSDPA" or "Topex Router" or "Wireless Broadband"

From the network adapters (network cards) of your computer, select the one which is connected via Wifi or Ethernet cable to the Bytton equipment.

In this example, it is the network board type
"3Com OfficeConnect".

Check the box "Internet Protocol (TCP/IP) and click the button "Properties" to configure your PC.

You may configure the connection to Bytton HSDPA either manually or automatically.



Automatic IP

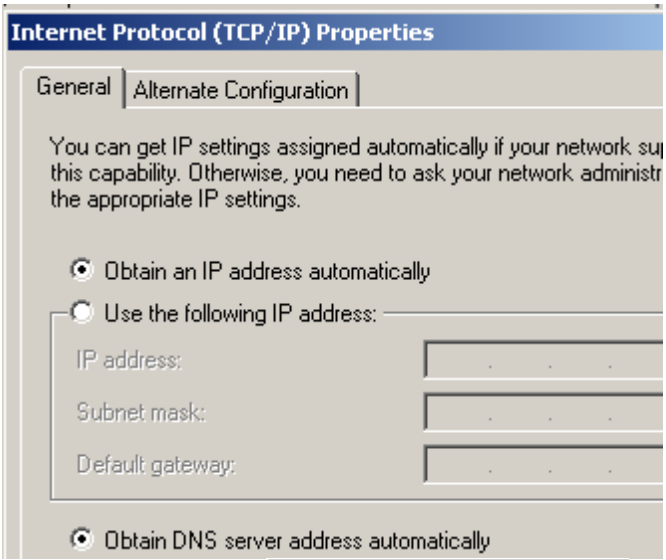
The simplest way is to set your network adapter to get its IP address automatically from BYTTON. The Topex HDSPA router features a DHCP server, so it can provide your PC with the correct IP address, DNS and Gateway.

In this case, in "Internet Protocol Properties" you should check the boxes:

- "Obtain an IP address automatically"
- and respectively "Obtain DNS server address automatically".

Reset (reboot) your PC to be sure these network settings become valid.

This way, you won't have to worry anymore about your settings, the Bytton 3G equipment will take care of providing your computer with adequate IP address and DNS.

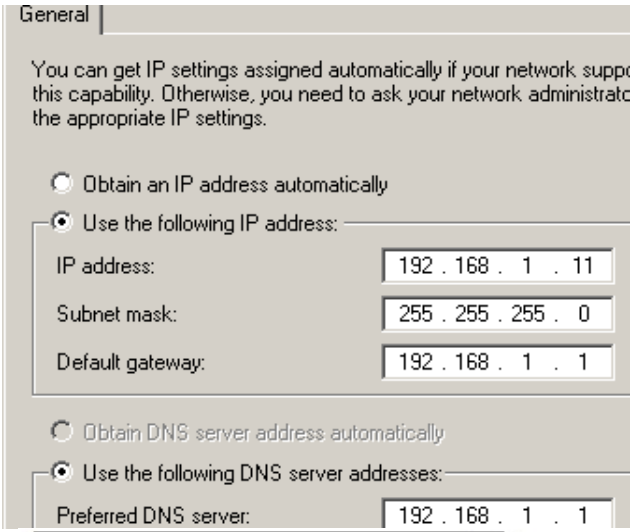

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network su
this capability. Otherwise, you need to ask your network administr
the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically

In the status bar at the bottom of the screen you should see the icon of the Bytton link blinking, and a first message will show up: "Bytton HSDPA acquiring network address" while the network adapter gets a local IP address.

Manual settings

As an alternative, you can set the network parameters manually. By default, Bytton ISDN has the IP address 192.168.1.1 and the standard Netmask 255.255.255.0, and these settings are used in the example below. However, it does not make sense to use manual settings for the *default configuration*, rather you should use manual settings if your local network has some special requirements, which the automatic configuration cannot satisfy.

In case of manual settings, in "Internet Protocol Properties" you must fill in the corresponding values:
- the IP address could be from 192.168.1.2 up to 192.168.1.254; to be sure you don't fall over the address of another device of your LAN, a value of 11 is suggested, instead of 2 which is the absolute minimum available value
- the Subnet mask must be the standard one, 255.255.255.0
- the Default gateway must be 192.168.1.1
- the same address 192.168.1.1 is to be used for the "Preferred DNS server"


General
You can get IP settings assigned automatically if your network supp
this capability. Otherwise, you need to ask your network administrat
the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 11
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 1 . 1

In the status bar at the bottom of the screen you should see the link icon blinking, and a message will show up: "Bytton HSDPA is now connected"

Note: ***When you use for your local network a Proxy Server, you must set an exception for the Topex wireless router, because otherwise you won't be able to access the BYTTON equipment!***

You should enter the IP address of the Bytton HSDPA device (by default 192.168.1.1) in the list of exceptions for the Proxy server: "Do not use proxy server for addresses beginning with …"

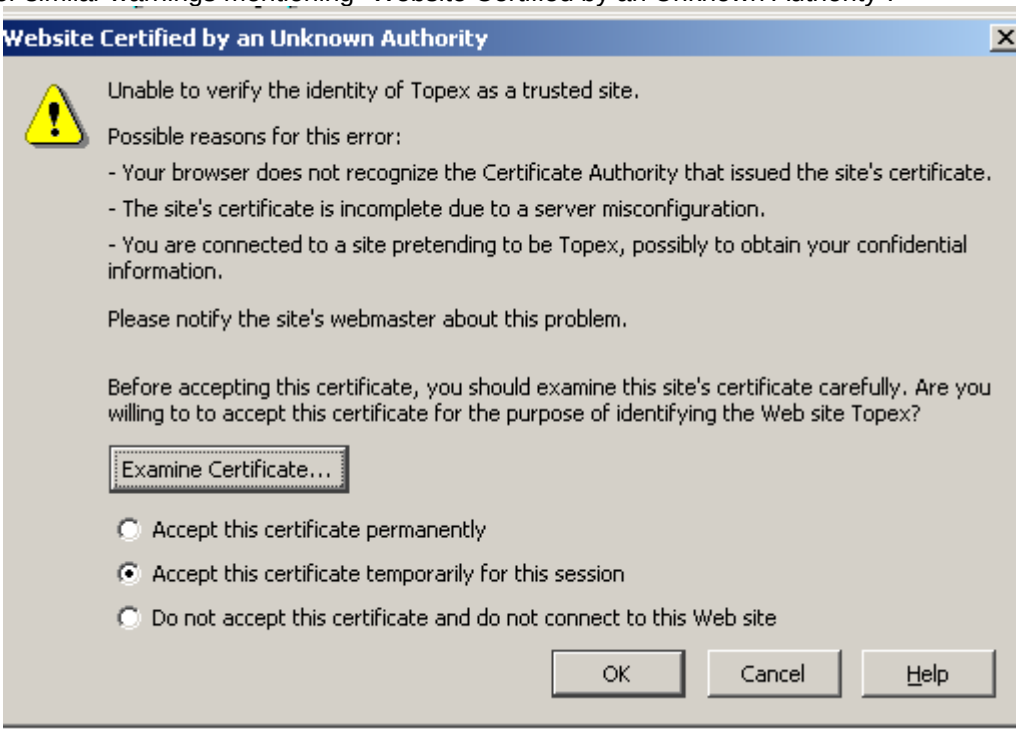
To configure the Bytton HSDPA product using the web interface, just open your favorite web browser and type the default IP address as the URL: https://192.168.1.1/ or enter directly the link for the Administrator pages: https://192.168.1.1/admin/

If you cannot connect to the BYTTON router because of problems in the settings of the IP address, you must go back to the factory default settings. Press the "RESET" button for at least three seconds. The equipment reboots and starts operating with the factory default settings, These include the IP address 192.168.1.1, allowing you to connect to the Topex wireless router in order to configure it. After reaching the configuration web pages, you may change the IP address of the device according to your requirements!

Note that BYTTON uses a **secure web connection** (https) so you may get several warning messages like this one:

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate has expired or is not yet valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

or similar warnings mentioning "Website Certified by an Unknown Authority":


Website Certified by an Unknown Authority
Unable to verify the identity of Topex as a trusted site.
Possible reasons for this error:
- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be Topex, possibly to obtain your confidential information.
Please notify the site's webmaster about this problem.
Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site Topex?
Examine Certificate...
Accept this certificate permanently
Accept this certificate temporarily for this session
Do not accept this certificate and do not connect to this Web site
OK
Cancel
Help

You should click „Yes", „OK" or „Accept" to go on.

Type "OK" to accept the certificate for the BYTTON website.
Other "Security Error" messages may warn you about "Domain Name Mismatch", referring to the security certificate. Again click "OK" to continue.

You may receive the warning "You have requested an encrypted page" or "You are about to view pages over a secure connection".

This is normal, it shows that you are connected to Bytton over a secure, encrypted link.

The secure connection is confirmed by the "padlock" symbol that shows up in the status bar at the bottom of the screen, indicating a secure (encrypted) connection. Bytton uses 128-bit SSL encryption to prevent hackers from capturing passwords and sensitive data. The same security is used by banks and the military.

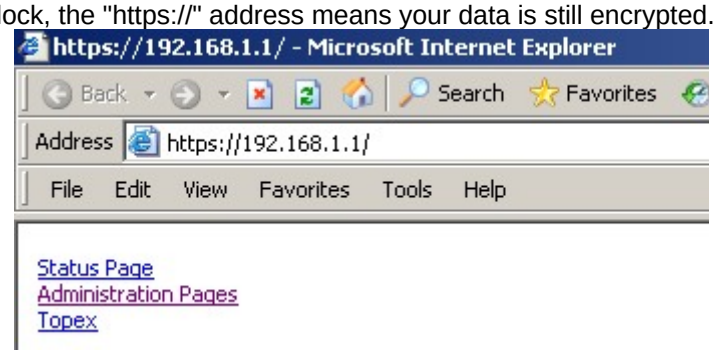
or

Internet Explorer shows the padlock icon only when everything on the entire webpage is encrypted. But even when the browser doesn't show a padlock, the "https://" address means your data is still encrypted.

From the fist configuration screen you may select either:

- status display
- configuration pages
- Topex webpage

Click the link of interest to you!

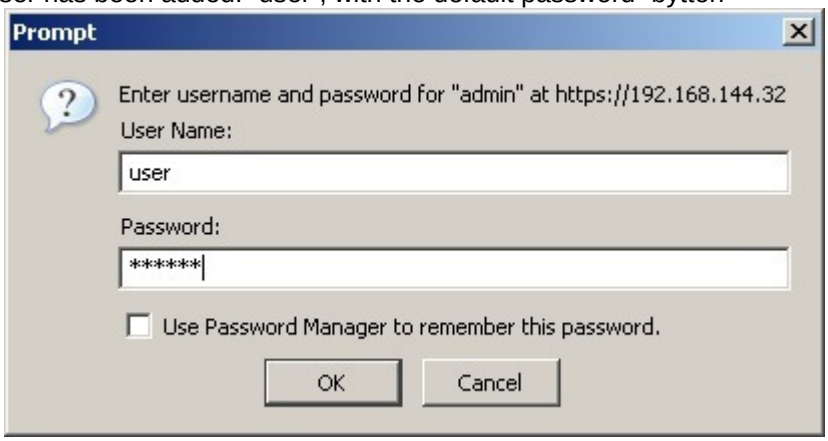


Now you will be asked to enter a user name and a password to access the configuration page of Topex BYTTON.

Multiple log-in options:

Starting with version 0.6.9, a new user has been added: "user", with the default password "bytton"

Now you may log-in either with the name "user" and the default password "bytton":



Or with the name "admin" and associated password "99admin11", as was done previously:

Correspondingly, you may change the password for each user.

For the administrator of the system network, the default user name is **admin** and the password is **99admin11**.
Later, you may change this password using the web configuration page, as described in the paragraph about Password.
For security reasons, it is strongly recommended to change as soon as possible the default password with one of your own choice. Also, you should NOT mark in your browser the checkbox "Remember my password".

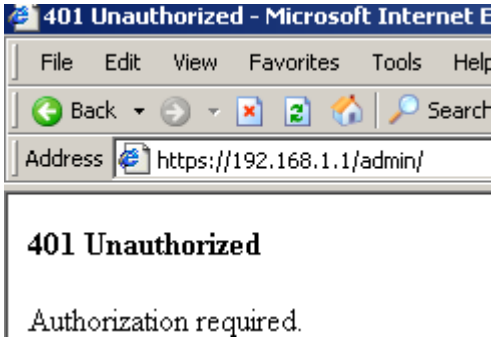
The log-in name is shown in the "Remote User" field, below the "Location" information:

The Administrator "admin" has more rights, access to additional settings, which a normal user does not require (advanced routing configurations and settings for drivers).

If you type a different user name, or if you enter an incorrect password more than three times in a row, you will get the error message:

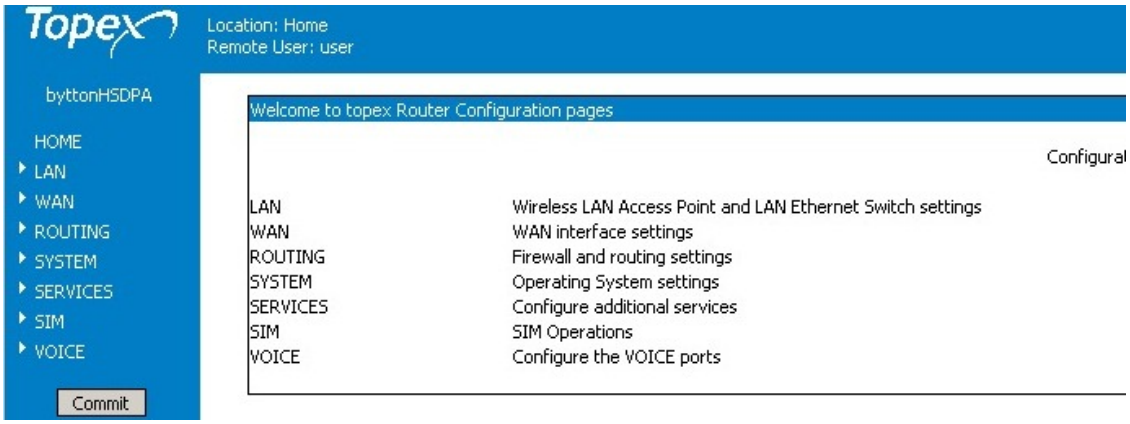
"401 Unauthorized" !

Connect again and be careful to enter the correct name and password.

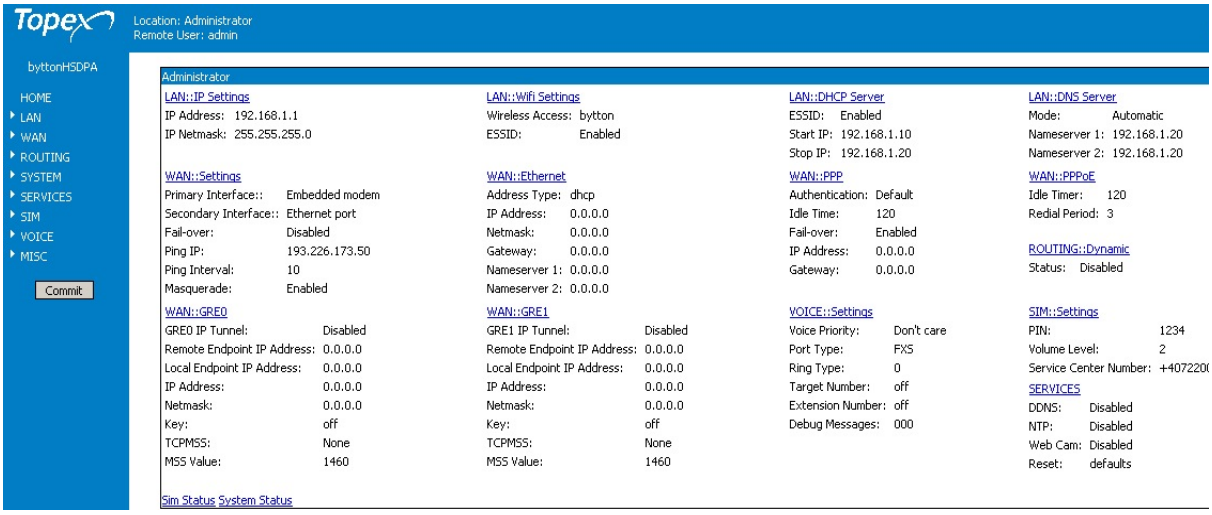


Following successful log-in, the main administration page for the Topex BYTTON router should be shown on screen.

Remember that the BYTTON home pages for User and respectively Admin will be slightly different, as shown next:
User:

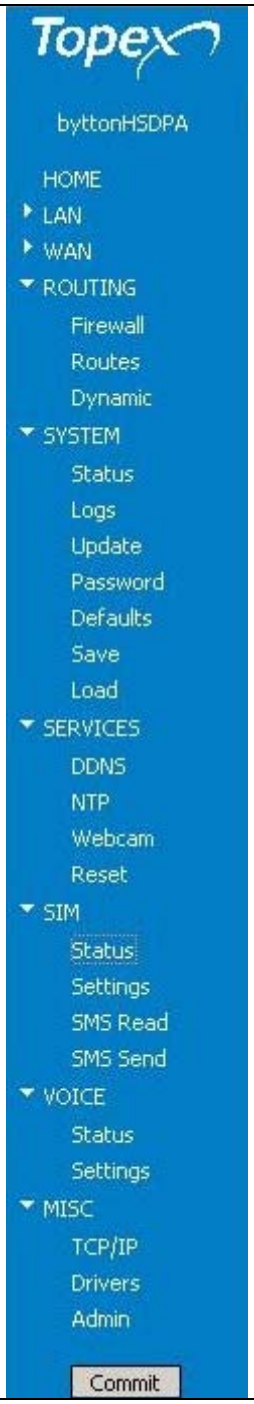


Administrator:

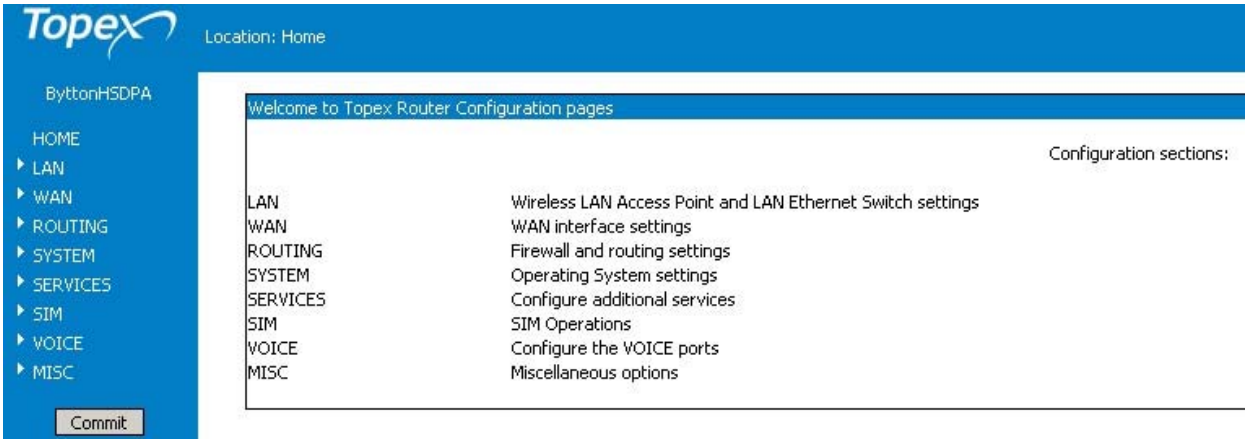


You notice that the admin has an additional configuration section, titled "MISC"

More, his homepage page is now structured with direct links to all the sub-pages of the web interface. This means that the administrator can click on the titles (colored in blue and underlined) to go directly to the respective sub-page in order to modify the settings.
Also, for each page of settings, the admin may see at a glance all of the current values.

User	Admin	Comments
		The additional menu item accessible when you log-in as Administrator is "MISC". The "Miscellaneous" section was created to include different advanced settings that are not required by a normal user, but may be need for a system administrator. Such settings may be: - TCP/IP, advanced networking parameters for the IP connection, for instance the ICMP redirects, and also the Host name to be used; - Drivers, detailed settings for different drivers, which are needed, for instance, when an external modem is used for the PPP link instead of the embedded HDSPA modem of BYTTON; - Admin, other settings related to the administration and management of the Bytton equipment.

After the configuration page is loaded, you can change any setting and then click the **Save** button to save it in the current page and **Commit** button to make these changes permanent.



There are several sections (Menu items) on the configuration page of BYTTON HSDPA, allowing you to modify the settings for:

- **HOME**: this home page for configuration of the equipment.
- **LAN**: settings for the wireless LAN (WiFi - embedded Access Point) and for the local wired (Ethernet) network
- **WAN:** parameters for Ethernet, PPP including AT commands, etc and Dynamic DNS
- **ROUTING:** routing**,** NAT (network address translation), firewall, etc.
- **SYSTEM:** Shows current status and performs operating system functions (update, change of password, logs)
- **SERVICES:** Allows you to configure additional services (such as DDNS, NTP or webcam
- **SIM:** Shows info and change settings for the SIM card and HSDPA module, allows viewing, sending out and receiving SMS messages
- **VOICE:** configuration of the telephony interfaces (FXO or FXS, ISDN etc)
- **MISC:** miscellaneous options for optimization (advanced settings). These are available only if you log-in as Administrator!

Depending upon the actual firmware version running on your Bytton ISDN router, you may or may not have access to all these configuration sections.

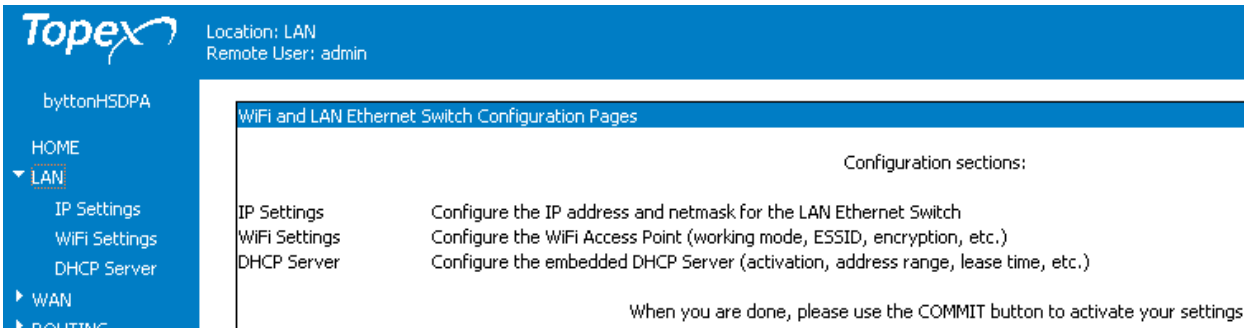
The Menu bar is located to the left, and features the button Commit at its bottom.
On top of the web page, after the Topex logo, you will see a "Location" indication, which reminds you where you are on the Web interface. In this example, the section is WAN and the subsection Settings.

Under the Location information you can see "Remote User", which shows you the name that was used for log-in, User or respectively Admin.

Note: *When you change the settings in any page, don't forget to press the "Save" button if you want to keep these settings. Otherwise, if you click any other link, you will reach another configuration page, and the new settings will be lost.*

5.2 LAN

This group features three pages of settings related to the local wireless or wired network (for IP, for the embedded WiFi access point and respectively for the DHCP server):


Location: LAN
Remote User: admin
byttonHSDPA
HOME
LAN
IP Settings
WiFi Settings
DHCP Server
WAN
WiFi and LAN Ethernet Switch Configuration Pages
Configuration sections:
IP Settings Configure the IP address and netmask for the LAN Ethernet Switch
WiFi Settings Configure the WiFi Access Point (working mode, ESSID, encryption, etc.)
DHCP Server Configure the embedded DHCP Server (activation, address range, lease time, etc.)
When you are done, please use the COMMIT button to activate your settings

5.2.1. IP Settings

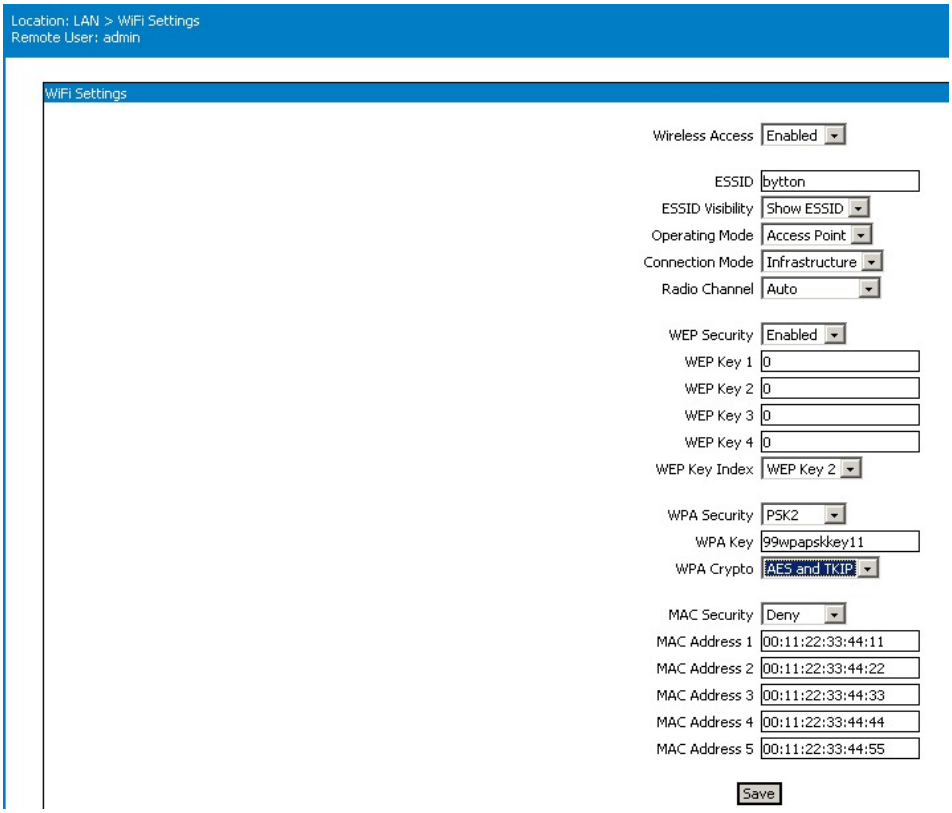
Settings for the LAN IP of the BYTTON HSDPA router are the standard ones: IP Address and Netmask. These settings control how the Topex equipment connects into your local wired (Ethernet) computer network.
The default address value is 192.168.1.1 and the netmask is 255.255.255.0.

You may change these default settings, if the configuration of your network requires this. Use the "Save" button to save the settings, then "Commit" (down on the column to the left of the screen) to make permanent the IP settings.

Usually the IP address allocated for BYTTON HSDPA on the LAN side is a **non-routable** (internal) address. If you change this IP address, you will need to reload the configuration page by typing the new IP address in your browser, if not redirected automatically.

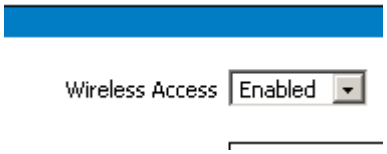
5.2.2. WiFi Settings

The settings for the wireless access point These control the 802.11b/g embedded Access Point (base station) of BYTTON HSDPA.

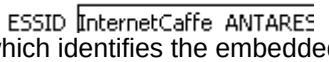


There are several zones (groups of WiFi related settings), which are described next.

Wireless access:
you may enable or disable the wireless access to the BYTTON HSDPA device. If you set it to **Disable**, the WiFi features will be inactive. To indicate this, all the following fields will be colored in gray, showing you that this section is inactive (you cannot perform changes here).

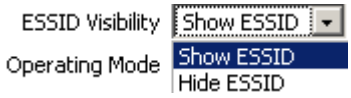


ESSID: name of the Wireless LAN.

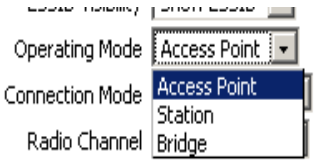


ESSID is a unique name, of length up to 32 keyboard characters, which identifies the embedded wireless Access Point of BYTTON in the wireless LAN. All devices in the wireless network must have the same ESSID. We strongly recommend changing the default.

ESSID Visibility: Shows or hides the ID, making your router visible/invisible to others. By default an ESSID is visible, meaning it is being broadcasted to all WiFi devices placed in its area, thus making the network prone intruders.

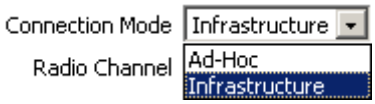


Operating Mode:
Access Point – standard mode of operation, BYTTON acts as a base station for several WiFi clients.
Station – BYTTON acts as a WiFi client, it connects to an existing Access Point.



Bridge – performs transparent bridging between two remote Access Points, also known as Wireless Distribution System(WDS) that allows connecting to several APs. It is most commonly as a WiFi repeater located midway between two Aps.

Connection Mode: It has two options, Infrastructure and Ad-Hoc.



Infrastructure: default operation mode. Several WiFi clients can connect to the BYTTON HSDPA, acting as server.

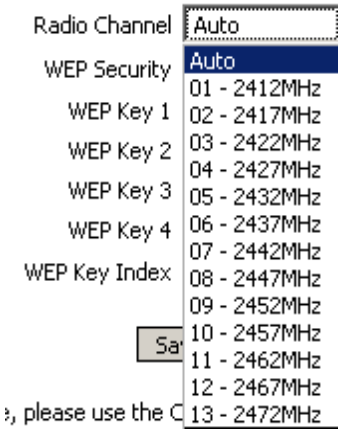
The "Infrastructure" mode takes full advantage of the AP's ability to cover wide areas.

Ad-Hoc: two wireless clients interconnect directly, without the need for an AP. In this connection mode, the BYTTON links directly to a computer with WiFi or an AP that is set to work in Ad-Hoc mode.

The "Ad Hoc" Mode is easier to set up, thus recommended for a very small or temporary network.

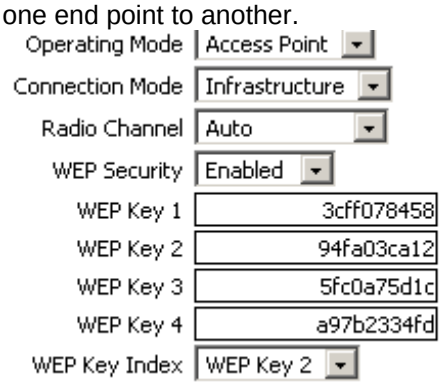
This setting is related to the previous one - usually, the "Ad-Hoc" connection is used when Operating Mode is set to "Station".

Radio Channel: Selects the WiFi channel in the 2400 MHz band.



In this band there are up to 14 channels, placed 5 MHz apart. Left on "Auto" (default setting) and the AP will automatically select the radio channel with the strongest signal. When selecting a certain channel, make sure all devices are broadcasting on the same channel.
This setting may be left on default, and changed only when experiencing interference with other devices.

WEP Security: Enables or disables WEP (Wired Equivalent Privacy) encryption.
WEP encryption is used to protect data transmitted from one end point to another.
The encryption level (64-bit or 128-bit) is given by the length of the WEP Key you enter.
If you enable WEP, these fields become active as shown here:



WEP Key 1 … 4: The data keys used for encryption/decryption. There are up to four keys, their values must be the same on the BYTTON Access Point and on the wireless stations connected to it. When using a 64-bit WEP encryption key, the password must be 5 characters long, and when using 128-bit WEP encryption key the password must be 10 characters long.

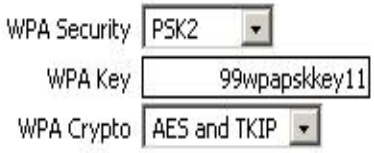
WEP Key Index: shows which key is active. You may have a list of pre-defined keys out of which the system administrator periodically chooses the active one. The selected WEP key is automatically published to the clients of the Access Point.

Warning: *WEP is a basic encryption method and it was designed to provide a level of privacy equivalent to an unsecured wired LAN, so you should not rely only on WEP for protection.*

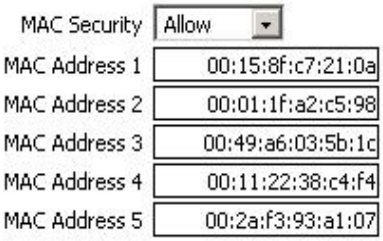
WPA sec: WPA security
Wi-Fi Protected Access, a Wi-Fi standard designed to improve the security features of WEP. It features improved data encryption through the temporal key integrity protocol (TKIP) and user authentication, through the extensible authentication protocol (EAP). EAP is built on a secure public-key encryption system to ensure that only authorized network users can access the WiFi network.
You can select to Disable the WPA security, or to use PSK or PSK2 keys. PSK means "pre-shared keys": the keys are public, every user is given the same passphrase.

The pre-shared key version is called WPA-Personal or WPA2-Personal, while the more secure version using 802.1X server authentication is WPA-Enterprise or WPA2-Enterprise.
In this case you must enter the respective key in the "WPA Key" field, the select the type of cryptography to be used for WPA:
You can select for cryptography TKIP, AES or both.

TKIP - Temporal Key Integrity Protocol is an enhanced data encryption technology that provides important data encryption enhancements, including a per-packet key-mixing function, a message integrity check (MIC), an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.
AES - Advanced Encryption Standard, which is an encryption algorithm highly recommended to ensure privacy of commercial transactions in the private sector.



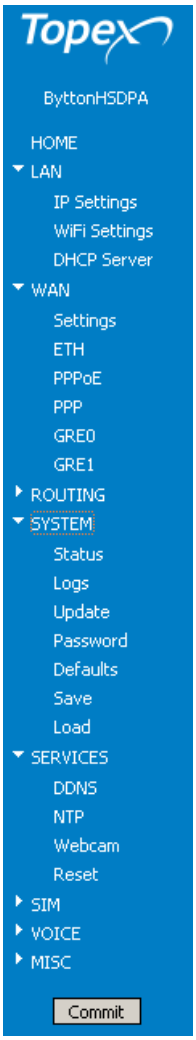
MAC Security
Controls access to the WiFi network based upon MACs (physical addresses of the client devices
By default MAC Security is Disabled, allowing any wireless client to connect, without checking its MAC-address.
You can enter up to five MAC addresses to be filtered by this kind of physical ID security.



Disabled: by default the MAC-based security feature is disabled, so the fields below are gray (inactive).
Allow: only users with the MAC addresses listed below will be allowed to join the local wireless network.
Deny: the users with the MAC addresses listed below will be denied access to the WiFi network.

Warning: *the filtering of MAC ID's is not a foolproof security solution, you should not rely only on it to ensure security for the WiFi network. MAC addresses over a network could be faked, unauthorized persons can use Identity Theft (MAC Spoofing) to simulate MAC ID's that are allowed to join the network.*

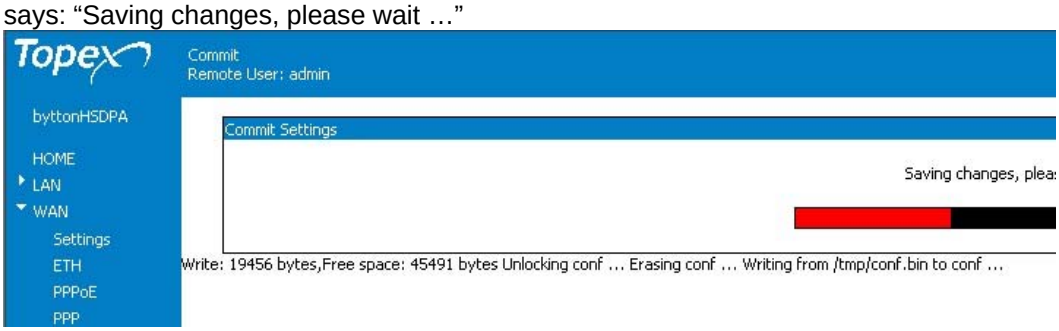
5.2.3. Commit



The "Commit" option described here is not specific to LAN, but rather it is a general option for the BYTTON equipment.
If you performed configuration changes, using the "Save" button is not enough since it saves the modifications only into the temporary memory.

You should always press the "Commit" button if you want to make these changes permanent.
This button is located at the bottom of the Menu list, to the left side of the screen.

You will see a "Commit Settings" message and, underneath it, a ed progress bar which says: "Saving changes, please wait …"

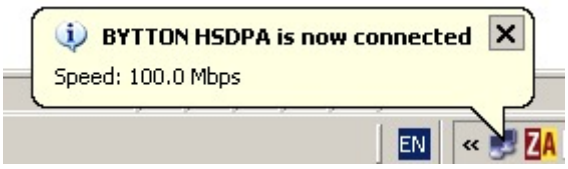


The message is really necessary, saving will take some times, because the changed settings are saved into permanent (Flash) memory of the equipment.
Under the progress bar other messages are shown, indicating the used and respective free memory of the equipment, and the stages of the operation: Unlocking, Erasing, Writing …
BYTTON resets, and when it starts again, the new set of parameters will be active.

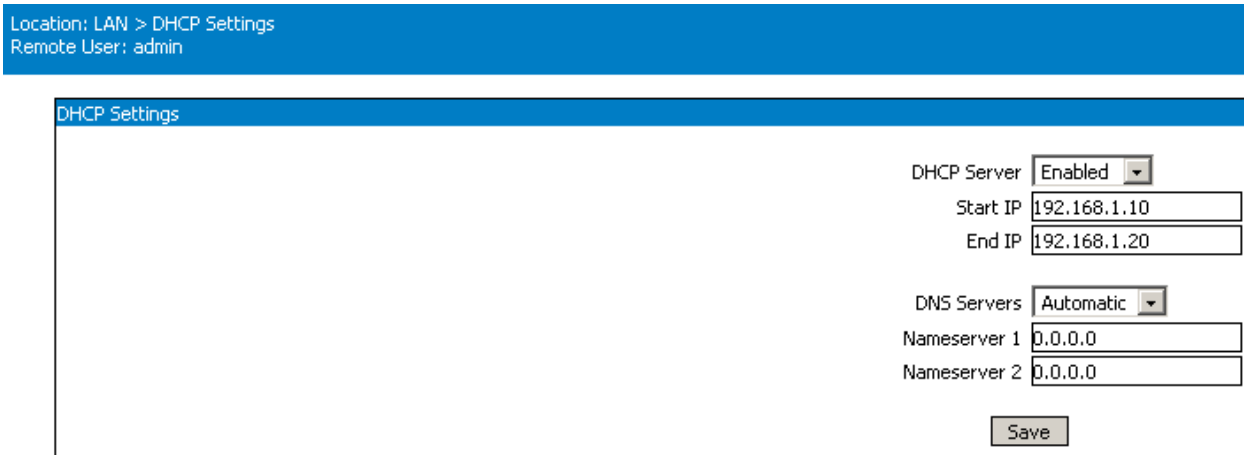
Warning! ***While committing changes, when resetting Bytton or while loading a new program image, the equipment will cease operation for a few seconds. This means all connections: data link, voice, LAN and WiFi will be interrupted, then will resume when BYTTON starts again.***

For instance, the status bar at the bottom of the screen will temporary indicate that the LAN connection with Bytton is not available ("cable unplugged" or "limited connectivity" message and connection icon with a red "x":

Then Bytton HDSPA restarts with the new parameters, and the LAN connection is immediately restored.



5.2.4. DHCP



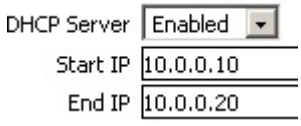
DHCP Server: Enabled or Disabled.
By default the Bytton HSDPA router acts as a DHCP server for the local network, thus dynamically assigning IP addresses to clients on the internal network. The Bytton HSDPA Wireless Router supports up to 254 IP addresses for your wireless network. When set to DISABLED IP addresses must be manually assigned by the network administrator.

Warning: *If you enable the DHCP feature of Bytton, make sure that there is no other DHCP server in your local network!*

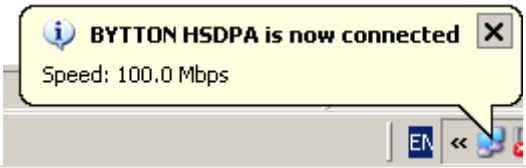
Start IP: Starting IP Address. The DHCP server allocates IP addresses in a user specified range (a pool of addresses). The Start option sets the **first** IP address in the pool.

End IP: End IP Address. The End option sets the **end** IP address, the last address in the pool to be assigned by the DHCP server in your local network.

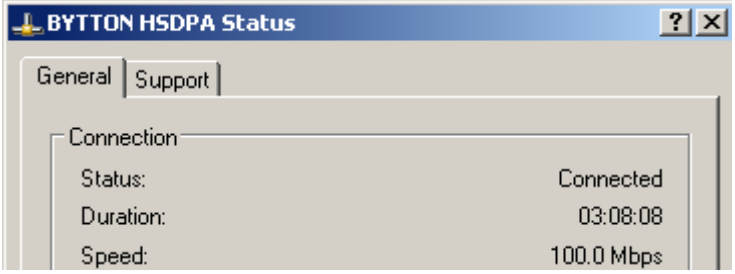
Note 1: *if the DHCP server is disabled, the fields below it, Start IP and End IP, will be displayed in grey. This shows you that the respective parameters are disabled.*
Note 2: *Remember that the default IP address of Bytton is 192.168.1.1, so the Start IP must be 192.168.1.2 or greater, but smaller than 192.168.1.254. You should set an adequate IP range for DHCP usage, for instance form 10 to 20 for a small network , or from 20 to 50 in case of a larger network.*
Note 3: *Of course, the DHCP setting must be correlated with the IP address of Bytton HDSPA. For instance, if the requirements of your network compel you to use an IP such as 10.0.0.1, instead of the default IP address "192.168.1.1." , the DHCP server must be also set for the* ***same range*** *of IP addresses, respectively:*



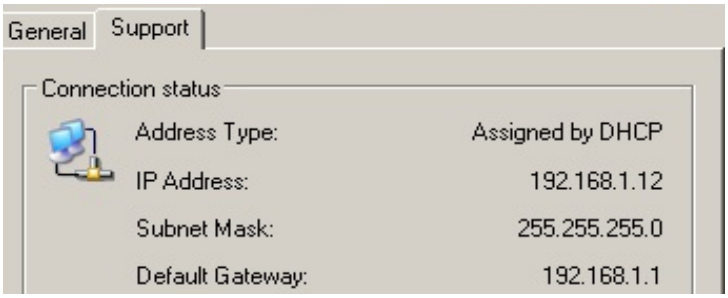
To check the correct assignment of IP address, double click the icon corresponding to the BYTTON network connection on the desktop of your computer.



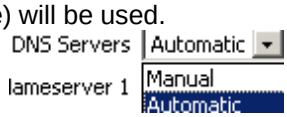
The Status window for the network connection will appear, as shown.
Click on the tab "Support" to see details about the network connection "BYTTON HSDPA":



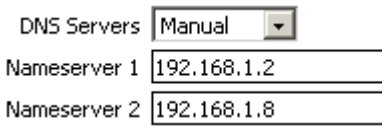
The "Support" window tells you that the IP address has been "Assigned by DHCP" and is in this example 192.168.1.12 (inside the range 10-20 that you have specified).
You can also verify that the default gateway is 192.168.1.1 (the BYTTON device) and the Subnet Mask is 255.255.255.0.



DNS Servers:
Select which primary and secondary servers for DNS (Domain Name Service) will be used.
Options are Automatic (default) and Manual.

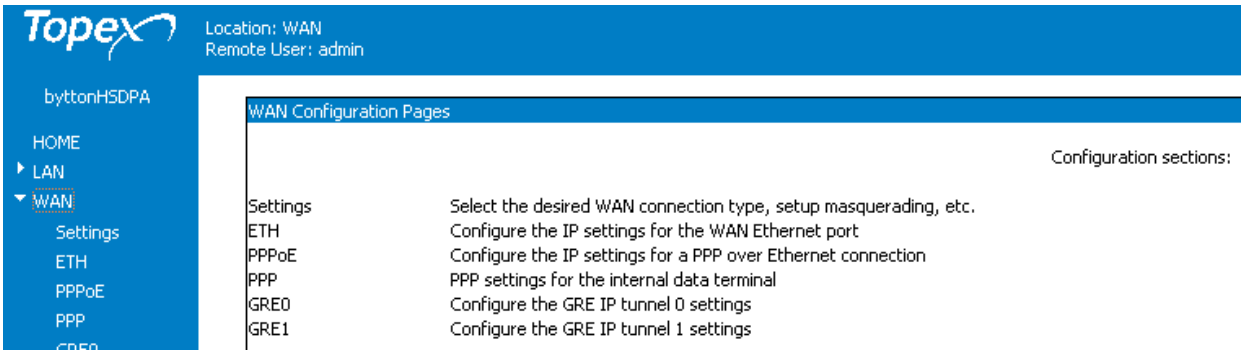


If you leave the setting to the default Automatic, the equipment will look for DNS servers in the local or remote networks.
Should you select the option "Manual", then you must complete the IP addresses of the Nameservers (primary and alternate) yourself.



5.3 WAN

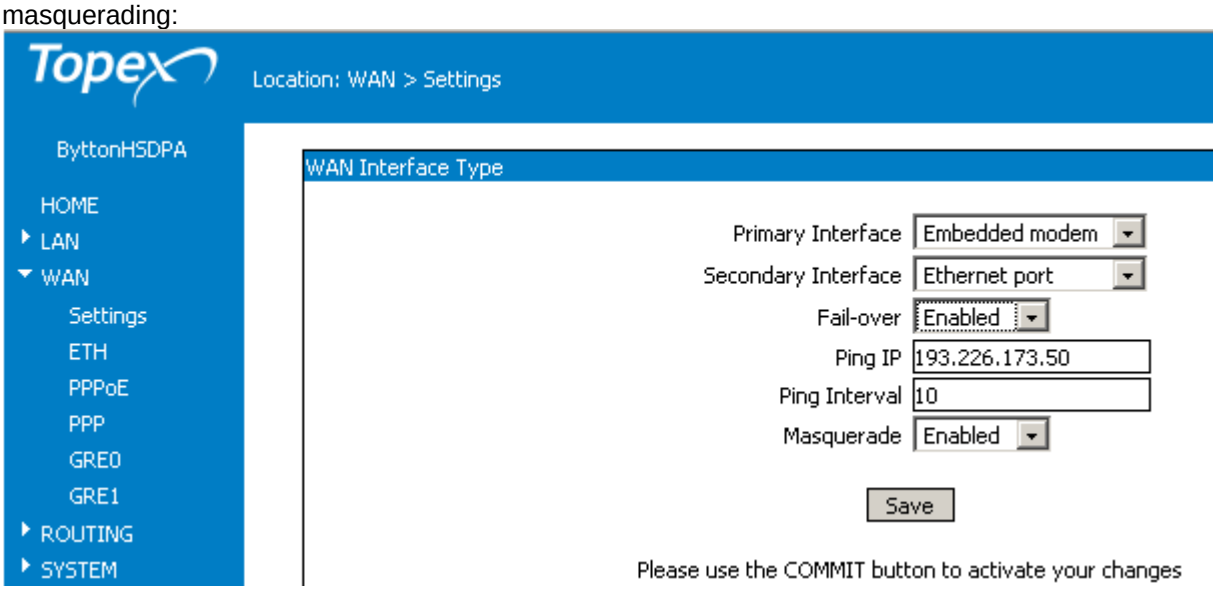
Here are the pages for configuring the WAN (remote network) side of the BYTTON router


Location: WAN
Remote User: admin
byttonHSDPA
HOME
LAN
WAN
Settings
ETH
PPPoE
PPP
WAN Configuration Pages
Configuration sections:
Settings Select the desired WAN connection type, setup masquerading, etc.
ETH Configure the IP settings for the WAN Ethernet port
PPPoE Configure the IP settings for a PPP over Ethernet connection
PPP PPP settings for the internal data terminal
GRE0 Configure the GRE IP tunnel 0 settings
GRE1 Configure the GRE IP tunnel 1 settings

The WAN Home-page brielfy describes your options in setting the WAN connection.

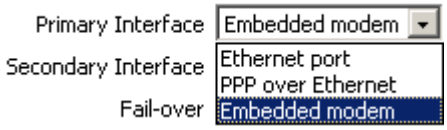
5.3.1. Settings

Allow you to select the type of the interface you use for WAN connection, the use of fail-over and of masquerading:



Primary Interface: You can select either:

- Embedded modem (PPP link)
- PPP over Ethernet (PPPoE)
- Ethernet Port

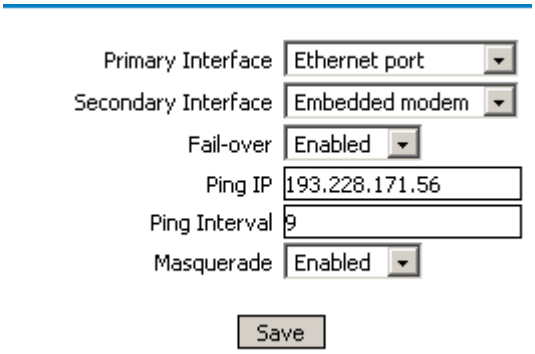


Secondary Interface: You can select either:

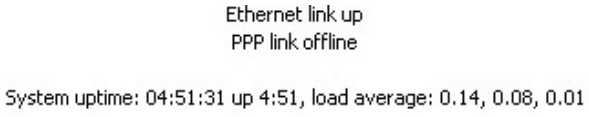
- Embedded modem (PPP link)
- PPP over Ethernet (PPPoE)
- Ethernet Port

You have **two** options for interfaces, primary and secondary. If the "Fail over" feature is enabled, when the primary WAN interface is no longer available, the Bytton HSDPA equipment automatically switches to the secondary interface.

Fail-over: if Enabled, the equipment will automatically switch from the primary WAN interface to the secondary interface, in case the main connection is broken . By default it is disabled.
Ping IP: an external address that will be periodically pinged. If it does not answer, Topex Bytton ISDN will decide whether the primary interface for the Internet is unavailable and it will switch to the secondary interface.
Ping Interval: the time period for pinging the respective address, for example ten seconds.
If the interval is too small, even a momentary interruption will cause the unneeded switching from the primary WAN interface to the alternate one. If period is too long, for some time there will be no Internet connection available (the primary WAN interface has failed but the secondary one has not yet been put in use).
Masquerade: Enable or Disable masquerading. Performs IP Masquerading or NAT (translation of source and destination IP addresses and port numbers upon data packets).
If the Internet provider that you connect to performs the masquerading at its location, you may leave this option Disabled.
Example:
In your office you have a local network with cable or DSL as WAN connection, which uses Bytton HDSPA as a backup link. You should set the Primary Interface to "Ethernet port" and the secondary one to the embedded mobile modem:



In normal operation all computers in your local network will reach the Internet via ETH port, so the Ethernet link is up and the PPP link (HDSPA modem) is disconnected:

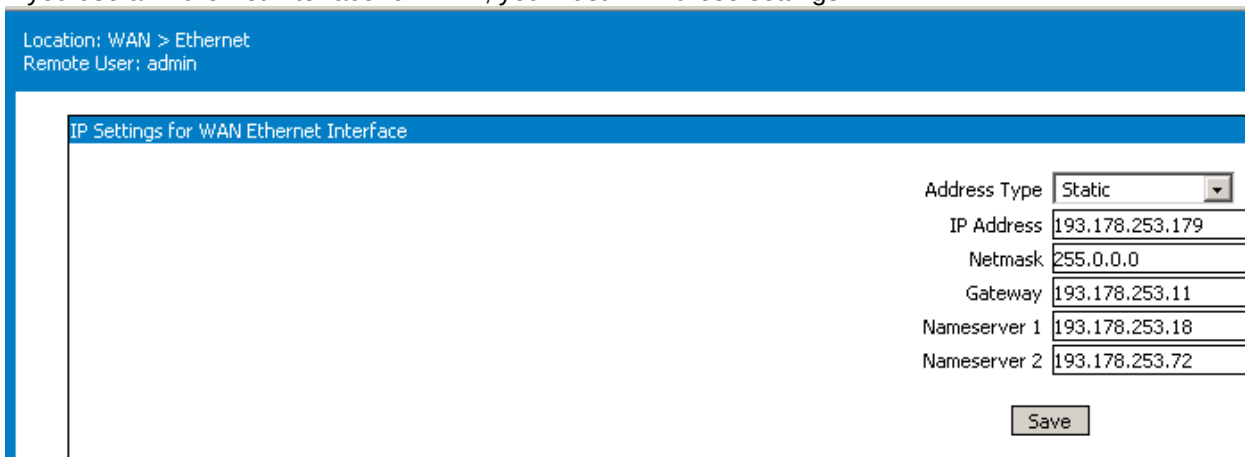


The routing is done via 192.168.0.0 gateway in the local network:

```
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.64.64.64     0.0.0.0         255.255.255.255 UH        0 0          0 ppp0
10.0.0.0        0.0.0.0         255.255.255.0   U         0 0          0 br0
192.168.0.0     0.0.0.0         255.255.0.0     U         0 0          0 vlan1
0.0.0.0         10.64.64.64     0.0.0.0         UG        0 0          0 ppp0
```

5.3.2. Ethernet

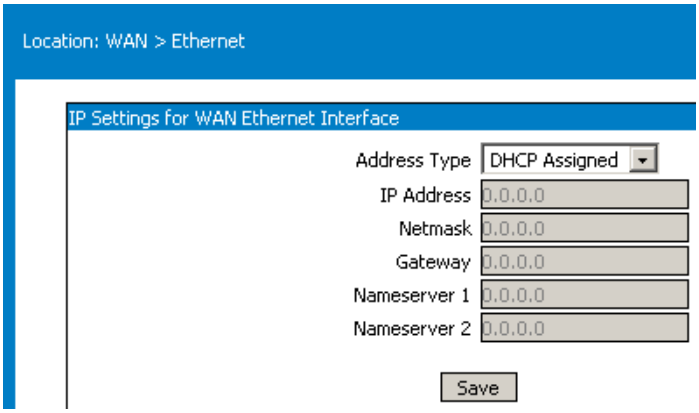
If you use an Ethernet interface for WAN, you must fill in these settings.



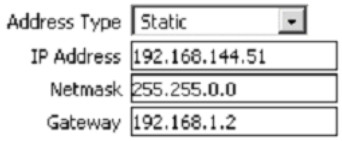
Address Type: options are Static or DHCP Assigned.

Default is "DHCP Assigned", which means that the IP address of the WAN Ethernet Interface will be automatically assigned by a DHCP server.

Note that in this case the fields below are inactive.

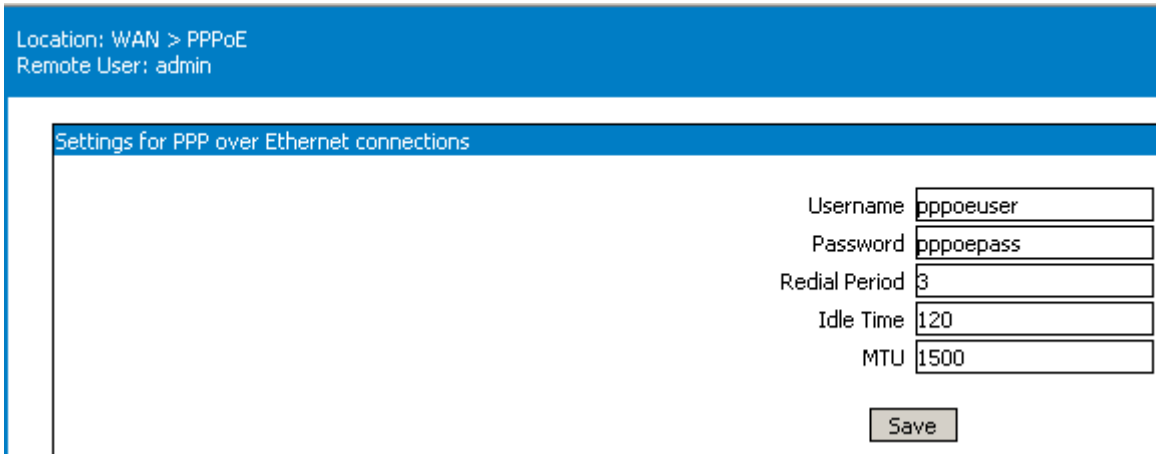


If you select "Static", then you must also fill in the: **IP Address** value on the WAN side, **Netmask**, **Gateway** address used for routing.



5.3.3. PPPoE

Settings for the connection using Point-to Point Protocol over the Ethernet. This may be used for instance if you connect to the Internet via an external DSL modem instead of the embedded HDSPA module.



Settings are the same as for "normal" PPP, except that the modem-related command strings are missing here.

Username: The user name used for log-in to the Internet account supplied by your ISP. Ask your Internet provider for details! Some Internet providers need the complete account name together with the hosting domain, the same as for an e-mail address: name@domain.eu, while other ISPs require that you type here just the name of your account.
Password: The password used for authenticating to your Internet account.
Redial Period: time in seconds until redialing a connection, if it was broken
Idle Time: BYTTON can disable the connection when there is no more data traffic. If no data packet is sent through the interface for a specified period of time, the Internet connection will be broken. This is useful in case of connections where you pay per connected time.
You can specify this time interval, in seconds. If the interval is too short, even a momentary lack of activity (no data traffic) will cause the Internet connection to be interrupted.
If you set the time interval to 0 (zero), the connection will remain always on, even if there is no data traffic on the remote interface.

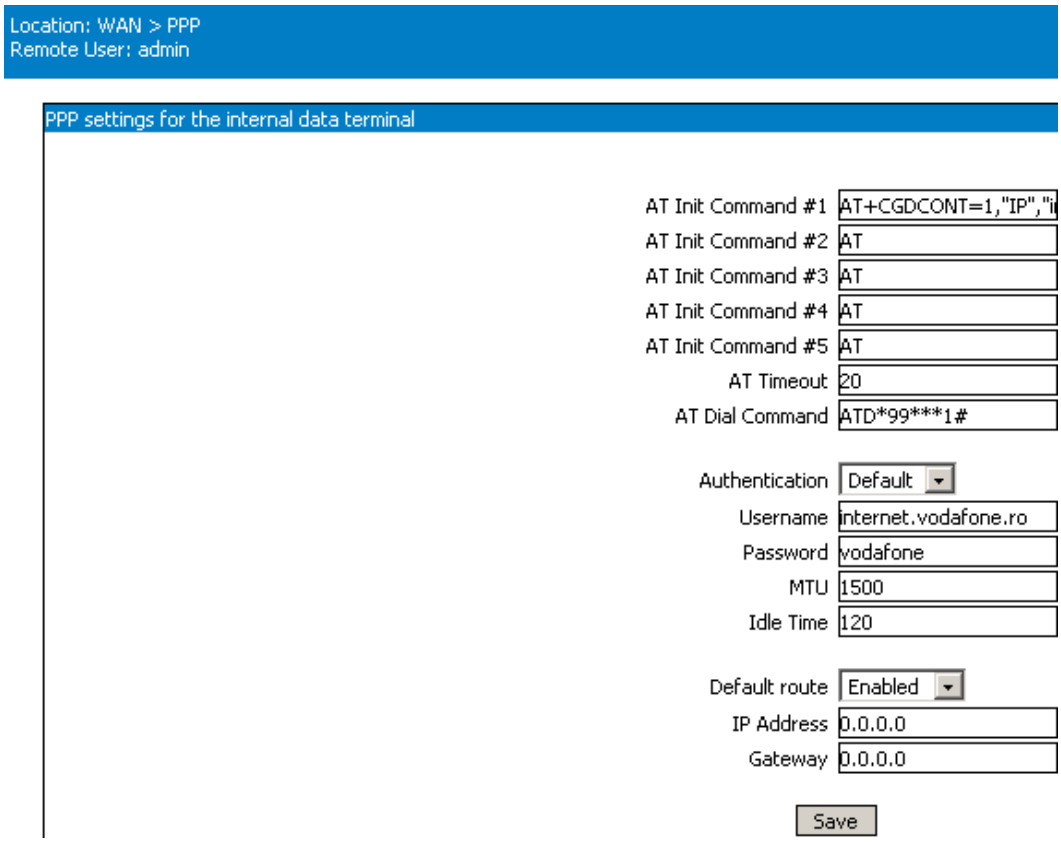
This feature is especially important for connections where you are charged for the total connection time, no matter the data traffic: to avoid unnecessary expenses, you should set BYTTON to disconnect when there is no data traffic.

MTU: value for the Maximum Transmission Unit. MTU is the largest physical packet size, measured in bytes, which a network can transmit. Messages larger than this will be fragmented into several packets. Different networks have different values for MTU, which is set by the network administrator. It is important to set the optimal MTU value, if it is incorrectly set the data transfers will be slow. The default MTU size is 576 for many PPP connections, 1024 for a modem connection, 1500 for Ethernet networks, etc. The same applies for MRU (maximum **receive** unit).

At the data level, the equivalent of MTU is MSS (see further on in the manual), so you must also set this parameter accordingly.

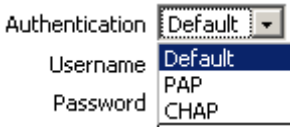
5.3.4. PPP

Settings for the PPP connection. To ensure high versatility, this page has several of configuration: for modem, for connection and for routing:



Modem settings:
This section controls the parameters of the Point-to-Point Protocol for the serial connection, in this case the embedded HSDPA modem. You need to change these settings when you go to a region with different settings, if you use a different network operator or when you replace the embedded HSDPA modem with another, external 3G modem that requires special parameters.
AT Init Command #1, 2, 3: Enter the character strings for the AT commands used to initialize the modem. Depending on the specifications of your 3G provider, you may need only one AT command or several.
AT Dial Command: Dial String, the AT command used to dial to the ISP, which includes the mobile phone number to be dialed. There are five "At Dial Command" fields. If there is no need to use all of them, fill the remaining with "AT". You should not leave empty fields in this section!

Connection settings
Parameters for the connection to the mobile Internet provider.
Authentication – allows you to select the method of authentication - you may leave it to Default, or force either PAP or CHAP.



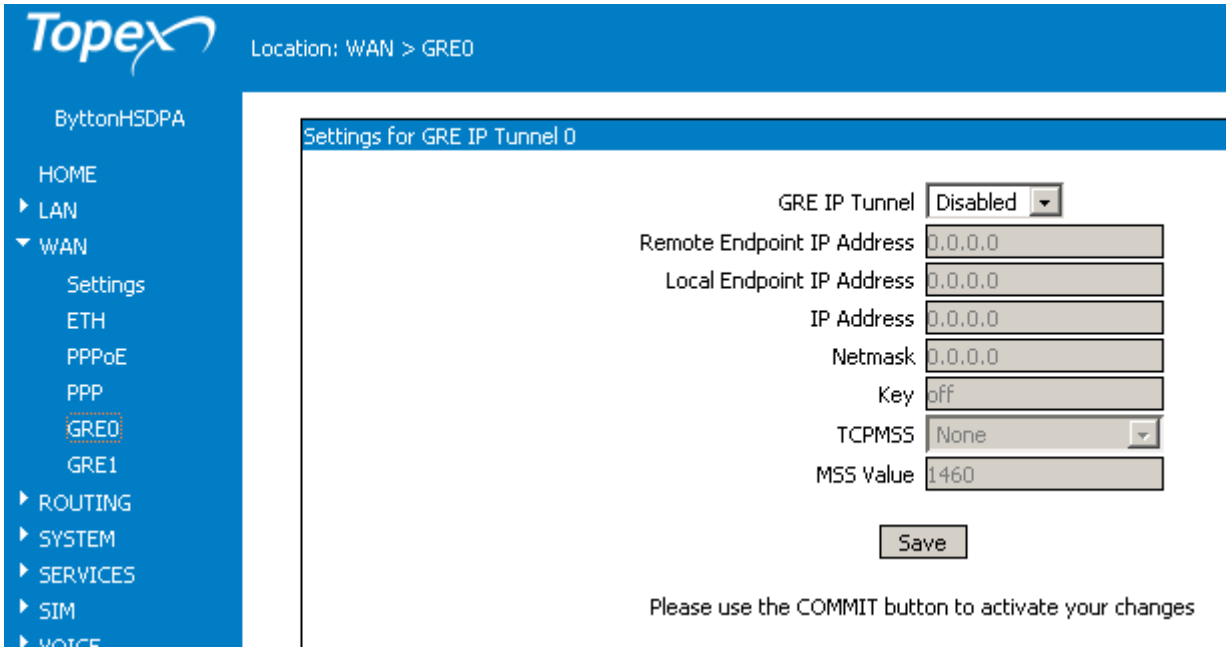
Default means it will authenticate upon request from the server, it accepts both PAP and CHAP, while
PAP means it will accept only PAP (password authentication), refusing CHAP, and
CHAP means it will accept CHAP (challenge authentication) and refuse PAP.

Username: The user name used for log-in to the 3G (UMTS or HDSPA) wireless network.
Password: The password used for authentication. You should ask your provider for these settings. Some network operators do not need username and password, log-in is allowed or not based upon Caller ID.
MTU: value for the Maximum Transmission Unit. MTU is the largest physical packet size, measured in bytes that a network can transmit. Messages larger than this will be fragmented into several packets. The MTUs should be the size of the reassembly buffer of the receiver, since you try to avoid fragmentation Different networks have different values for MTU, which is set by the network administrator. The default MTU size is 576 for many PPP connections, 1500 for Ethernet networks, etc.
Idle Time: BYTTON can disable the dial-up connection when there is no more data traffic. If no data packet is sent through the 3G link, the Internet connection will be broken. You can specify this time interval, in seconds. If you set the time interval to 0 (zero), the dial-up connection will remain always on, even if there is no data traffic on the remote interface.
When it detects outgoing data traffic, BYTTON automatically performs dial-up, in order to connect to the Internet.

Route:
Default route: Disabled or Enabled. This new feature, allows you to ask the Internet provider for a static address. Usually, the ISP assigns you the first available address each time you connect. Now you have the options either to accept the dynamic address assigned by DHCP or to ask for a specific static address. In this case you must fill the other parameters as well:
IP Address, **Gateway**, and the **Name servers** (primary and secondary) to be used.

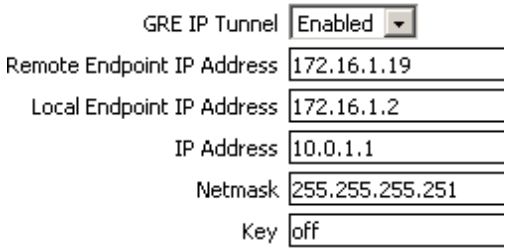
5.3.5. GRE

Settings for the GRE IP Tunnel, which is used when you need to perform IP tunneling in order to achieve a Virtual Private Network using several BYTTON HSDPA devices interconnected over the 3G mobile communications network.



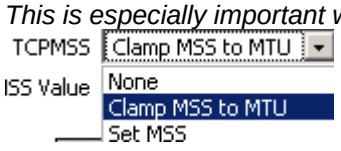
GRE IP Tunnel0: select Enable or Disable.
The default is Disabled, meaning that IP tunneling is not used.

When GRE IP tunneling is Enabled, the fields will be active, for you to fill-in their corresponding values.
Remote Endpoint IP Address: the IP address of the remote end of the tunnel.
Local Endpoint IP Address: the IP address of the local end of the tunnel.
Local IP Address: the IP address and netmask of the interface on which the tunnel is raised
static local address and its corresponding Netmask



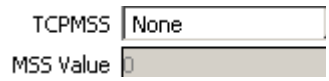
Key: the "key" code required for establishing a GRE IP tunnel.
This is a security feature, using a proprietary application: the remote endpoint won't accept tunneling connections unless it "knows" their keys. This way, if unauthorized persons know your GRE settings but do not have the code for the key, they won't be able to establish an IP tunnel.
By default the Key field has the value "off", meaning no tunnel key is used.

TCPMSS and MSS
TCPMSS is the option for the TCP maximum segment size in transmission and reception.
MSS is the Maximum Segment Size, the maximum amount of data that can be contained in a TCP packet (that may be handled by a network in a single, unfragmented piece). To reach optimum communications, you must set the correct value for MSS, which is related to the size of the maximum transmission unit (MTU) for the respective connection.
This is especially important when you use tunneling.



TCPMSS options are:
- none (Bytton does not set the TCPMSS value)
- Clamp MSS to MTU (MSS follows the value of MTU)
- Set MSS (you set manually the MSS value).

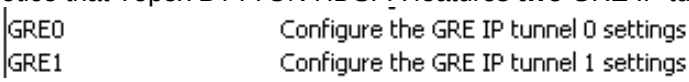
For the first two values, the field "MSS Value" is inactive.



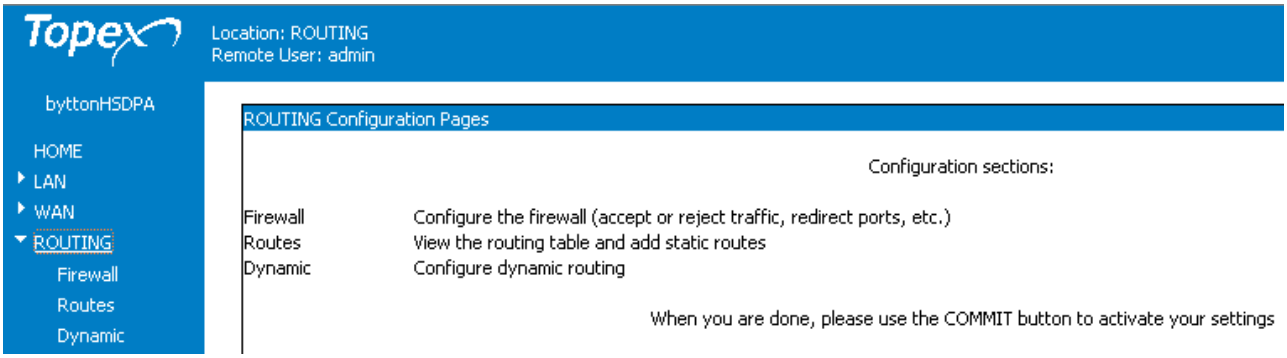
Clamping means MSS = MTU – 40 (MSS is only the size of TCP data that doesn't include the 20 byte TCP header and the 20 byte IP header).
Thus for the Ethernet link the MSS value would be 1460, since MTU is 1500.

If you selected "Set MSS", the field below it, "MSS Value", becomes active, it is no longer gray, now you can enter here the value for MSS.

Notice that Topex BYTTON HDSPA features **two** GRE IP tunnels, GRE0 and GRE1.



5.4 ROUTING



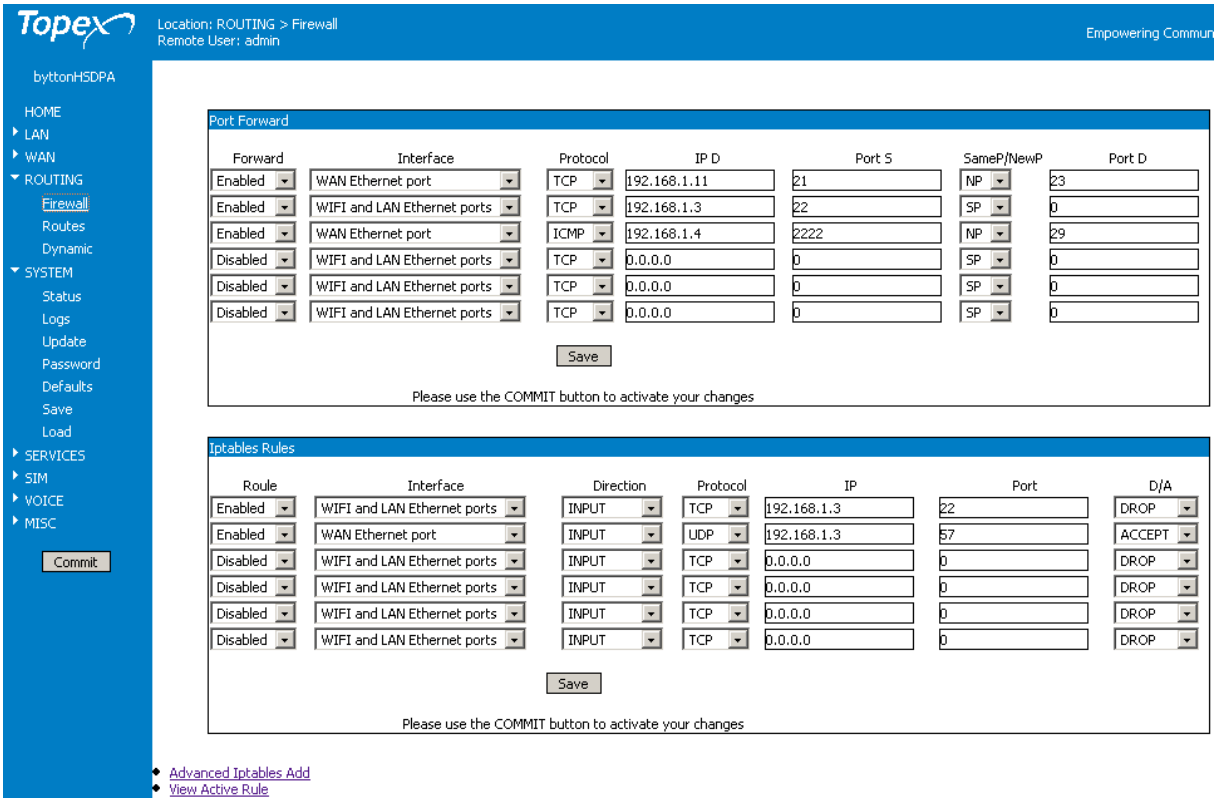
The section about "ROUTING" includes thee sub-sections:

- Firewall (both packet filtering and port or address redirection)
- Routes (display and configure the static routes)
- Dynamic (selects OSPF or RIP for dynamic routing).

5.4.1. Firewall

BYTTON HSDPA comes with a default firewall configuration, which ensures the security of your local network.

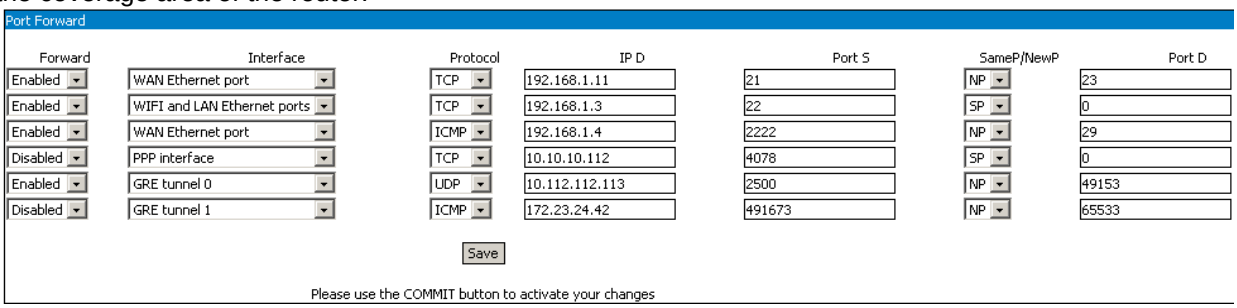
The "Firewall" section includes both NAT (redirecting addresses), port forwarding (PAT) and Firewall (accepts or rejects data packets). Thus the BYTTON Firewall configuration page features two sections: upper pane "Port Forward" and lower pane "Iptables Rules" and two clickable links, "Advanced Iptables" and respectively "View Active Rules", which will open additional sections.


Topex
Location: ROUTING > Firewall
Remote User: admin
Empowering Commun
byttonHSDPA
HOME
LAN
WAN
ROUTING
Firewall
Routes
Dynamic
SYSTEM
Status
Logs
Update
Password
Defaults
Save
Load
SERVICES
SIM
VOICE
MISC
Commit
Port Forward
Forward Interface Protocol IP D Port S SameP/NewP Port D
Enabled WAN Ethernet port TCP 192.168.1.11 21 NP 23
Enabled WIFI and LAN Ethernet ports TCP 192.168.1.3 22 SP 0
Enabled WAN Ethernet port ICMP 192.168.1.4 2222 NP 29
Disabled WIFI and LAN Ethernet ports TCP 0.0.0.0 0 SP 0
Disabled WIFI and LAN Ethernet ports TCP 0.0.0.0 0 SP 0
Disabled WIFI and LAN Ethernet ports TCP 0.0.0.0 0 SP 0
Save
Please use the COMMIT button to activate your changes
Iptables Rules
Roule Interface Direction Protocol IP Port D/A
Enabled WIFI and LAN Ethernet ports INPUT TCP 192.168.1.3 22 DROP
Enabled WAN Ethernet port INPUT UDP 192.168.1.3 57 ACCEPT
Disabled WIFI and LAN Ethernet ports INPUT TCP 0.0.0.0 0 DROP
Disabled WIFI and LAN Ethernet ports INPUT TCP 0.0.0.0 0 DROP
Disabled WIFI and LAN Ethernet ports INPUT TCP 0.0.0.0 0 DROP
Disabled WIFI and LAN Ethernet ports INPUT TCP 0.0.0.0 0 DROP
Save
Please use the COMMIT button to activate your changes
Advanced Iptables Add
View Active Rule

Note that each of the two panes has its own "Save" button, allowing you to save independently the two groups of settings.

Port forward

This section allows the forwarding of firewall ports from the Bytton equipment to a local computer from the coverage area of the router.


Port Forward
Forward Interface Protocol IP D Port S SameP/NewP Port D
Enabled WAN Ethernet port TCP 192.168.1.11 21 NP 23
Enabled WIFI and LAN Ethernet ports TCP 192.168.1.3 22 SP 0
Enabled WAN Ethernet port ICMP 192.168.1.4 2222 NP 29
Disabled PPP interface TCP 10.10.10.112 4078 SP 0
Enabled GRE tunnel 0 UDP 10.112.112.113 2500 NP 49153
Disabled GRE tunnel 1 ICMP 172.23.24.42 491673 NP 65533
Save
Please use the COMMIT button to activate your changes

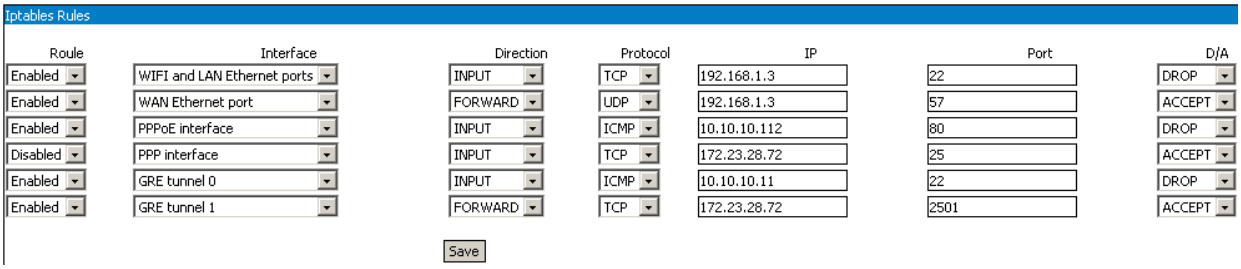
- **Forward** – select **"Enabled"** to activate the port forward operation. If you leave the default setting "**Disabled**", the port forwarding cannot be achieved;
- **Interface** – select the type of the used interface in order to communicate with the Bytton equipment. The available options are:
  - WiFi and LAN Ethernet ports – the local (wireless or wired) ports of Bytton;
  - WAN Ethernet port – the WAN port;
  - PPP interface – the mobile (UMTS / HSDPA) connection;
  - GRE tunnel 0, GRE tunnel 1 – the GRE IP tunnel.
- **Protocol** – select the IP protocol. **TCP** and **UDP** protocols are used for communications, while the **ICMP** protocol is for the "ping" command;
- **IP D** – The IP Destination field. It contains the IP address of the computer where the firewall ports will be forwarded. If you enabled rule but leave the Ipto the default "0.0.0.0", then no rule will be added to iptables.
- **Port S** – The source port – represents the number of the port that will be forwarded;

- **Same P / New P** – This section allows you to select two options:
  - **SP** – when this option is selected the source port typed in the Port S field will be forwarded on the **same port** to the computer with the IP address from the IP D field. If you select the "SP" option, the "Port D" field will be filled only with the 0 value;
  - **NP** – if you select this option, you will have to fill the "**Port D**" area with the number of the **new** port to which you want to forward the port from the "Port S" field.
- **Port D** – the destination port. This area is filled when the "NP" option is selected in the "Same P / New P" section. It represents the number of port where the source port is forwarded.

After you select these options press the "**Save**" and "**Commit**" buttons.

Iptables rules

This section allows setting rules for the iptable via the web interface.



- **Rule** – enables or disables the rule for the iptables
- **Interface** - select the type of the used interface in order to communicate with the Bytton equipment. The available options are the same as for the **Port forward** section;
- **Direction** – select "Input" to open a communication link or "Forward" to redirect the source port from the Bytton equipment;
- **Protocol** – select the communication protocol used. The options are TCP, UDP or ICMP;
- **IP** – the IP address of the computer from the coverage area of the Bytton, in the case when in the "Direction" field is set "Forward". When it is set the "Input" option the IP address will not be filled;
- **Port** – the number of source port which will be open;
- **D/A** – accept or drop the respective rule.***View Active Rules***

In this page you can see the active rules for the firewall, rules that you have set in the previous section.

General info:
The firewall has several sections, for pre-routing, post-routing, input, output and forwarding of data packets. This refers to the moment of time for the data packets:
PREROUTING: before effective routing, as soon as the packets are received by an interface.
POSTROUTING: after the local routing is performed, but before *leaving* an interface
INPUT: Right before they are sent a local process, the rules apply to external packets that are sent to the equipment.
OUTPUT: Right after they are generated by a local process, rules apply to packets that et out of the BYTTON router.
FORWARD: transfer operations, the data packets are coming in through one interface and getting out via another interface.

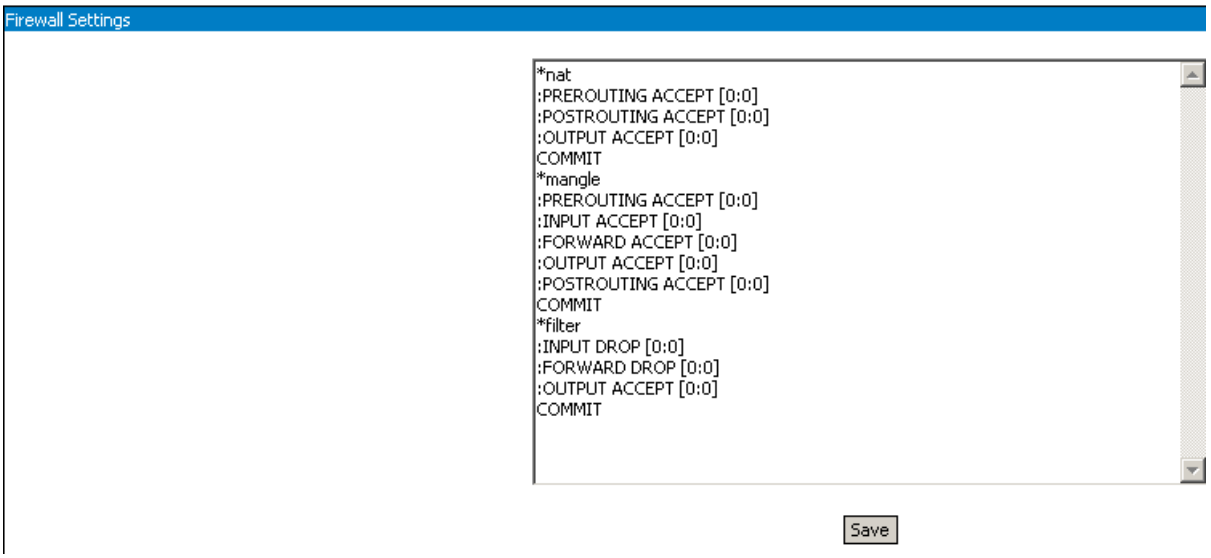
```
:OUTPUT ACCEPT [0:0]
-A INPUT -i lo -j ACCEPT
-A INPUT -i br0 -p icmp -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i br0 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -i br0 -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -i br0 -p tcp -m tcp --dport 443 -j ACCEPT
-A INPUT -i br0 -p tcp -m tcp --dport 3128 -j ACCEPT
-A INPUT -i br0 -p tcp -m tcp --dport 3129 -j ACCEPT
-A INPUT -i br0 -p tcp -m tcp --dport 1110 -j ACCEPT
-A INPUT -i br0 -p tcp -m tcp --dport 1025 -j ACCEPT
-A INPUT -i br0 -p udp -m udp --dport 67:68 -j ACCEPT
-A INPUT -i br0 -p udp -m udp --dport 53 -j ACCEPT
-A INPUT -i ppp0 -p udp -m udp --sport 53 -j ACCEPT
-A FORWARD -i br0 -o br0 -j ACCEPT
-A FORWARD -i br0 -o ppp0 -j ACCEPT
-A FORWARD -i br0 -o vlan1 -j ACCEPT
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -p tcp -m tcp --tcp-flags SYN,RST SYN -j TCPMSS --clamp-mss-to-pmtu
COMMIT
```

Active Rules:

Firewall view rule

```
# Generated by iptables-save v1.3.3 on Sat Jan  1 00:03:32 2000
*nat
:PREROUTING ACCEPT [30:2337]
:POSTROUTING ACCEPT [23:1472]
:OUTPUT ACCEPT [31:1912]
-A PREROUTING -i vlan1 -p tcp -m tcp --dport 21 -j DNAT --to-destination 192.168.1.11:23
-A PREROUTING -i br0 -p tcp -m tcp --dport 22 -j DNAT --to-destination 192.168.1.3:22
-A PREROUTING -i gre0 -p udp -m udp --dport 2500 -j DNAT --to-destination 10.112.112.113:49153
-A POSTROUTING -o vlan1 -j MASQUERADE
-A POSTROUTING -o ppp1 -j MASQUERADE
-A POSTROUTING -o ppp0 -j MASQUERADE
COMMIT
# Completed on Sat Jan  1 00:03:32 2000
# Generated by iptables-save v1.3.3 on Sat Jan  1 00:03:32 2000
*mangle
:PREROUTING ACCEPT [562:38620]
:INPUT ACCEPT [557:38057]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [631:181504]
:POSTROUTING ACCEPT [631:181504]
COMMIT
# Completed on Sat Jan  1 00:03:32 2000
# Generated by iptables-save v1.3.3 on Sat Jan  1 00:03:32 2000
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [631:181504]
-A INPUT -i lo -j ACCEPT
-A INPUT -i br0 -j ACCEPT
-A INPUT -p gre -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -d 192.168.1.3 -i br0 -p tcp -m tcp --dport 22 -j DROP
-A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 2222 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 2601 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 2604 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 3000 -j ACCEPT
-A FORWARD -i br0 -j ACCEPT
-A FORWARD -p gre -j ACCEPT
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -p tcp -m tcp --tcp-flags SYN,RST SYN -j TCPMSS --clamp-mss-to-pmtu
-A FORWARD -d 192.168.1.11 -p tcp -m tcp --dport 23 -j ACCEPT
-A FORWARD -d 192.168.1.3 -p tcp -m tcp --dport 22 -j ACCEPT
-A FORWARD -d 10.112.112.113 -p udp -m udp --dport 49153 -j ACCEPT
-A FORWARD -d 192.168.1.3 -i vlan1 -p udp -m udp --dport 57 -j ACCEPT
-A FORWARD -d 172.23.28.72 -i gre1 -p tcp -m tcp --dport 2501 -j ACCEPT
-A OUTPUT -p tcp -m tcp --tcp-flags SYN,RST SYN -j TCPMSS --clamp-mss-to-pmtu
COMMIT
# Completed on Sat Jan  1 00:03:32 2000
```

Advanced Iptables Add
This link provides you access to a console where you can add and edit rules for routing:



The firewall and advanced packet routing can be configured using the *iptables* commands. For more information, see http://www.netfilter.org.

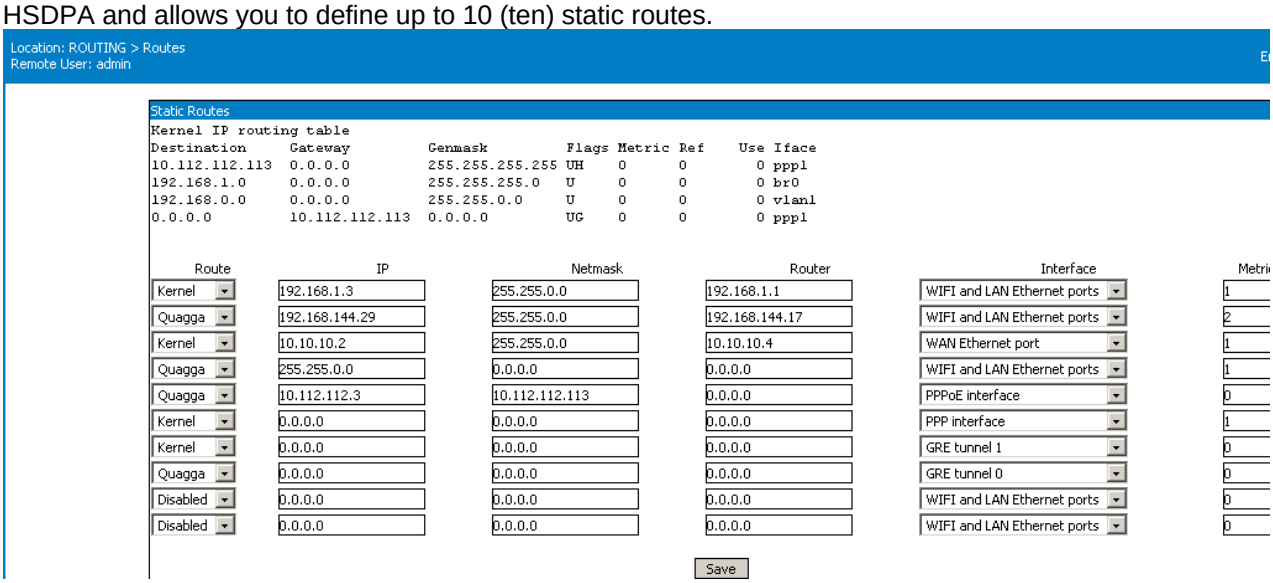
Warning! *Please remember that if you change the default values you may compromise your network security by allowing entrusted access. These configuration options need an advanced level of knowledge regarding network security and Linux kernel packet handling.*

Note : As you may see, the visible settings of the NAT/firewall configuration page are quite few. This happens because the basic rules for address translation and packet filtering **are already defined**, and they are not directly accessible to the user. Since they can't be changed, they are not visible!

What you see are the additional rules, the ones that you are allowed to modify, to supplement or delete. The firmware of BYTTON HSDPA automatically installs the basic rules that are required. For instance, if you enable the Webcam feature, the firmware opens the port 2000 for TCP traffic, if you enable the NTP service it opens port 123 for UDP traffic, and so on.

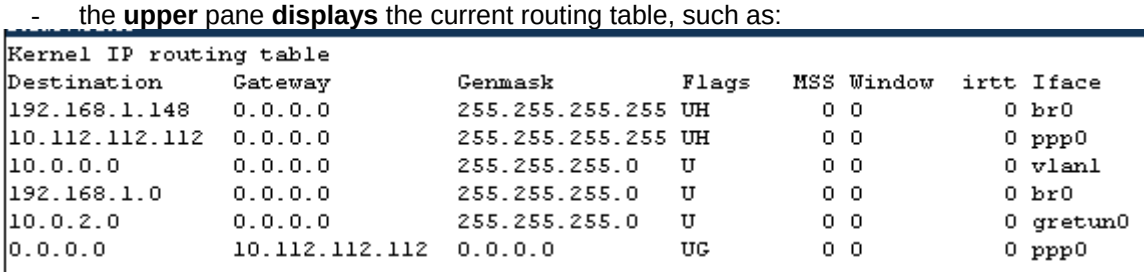
5.4.2. Static Routes

Routing means determining and prescribing the path or method used for forwarding data packets. This option page is concerned with fixed (static) routes. It shows the current routing table for BYTTON HSDPA and allows you to define up to 10 (ten) static routes.


Location: ROUTING > Routes
Remote User: admin
Static Routes
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
10.112.112.113 0.0.0.0 255.255.255.255 UH 0 0 0 ppp1
192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 br0
192.168.0.0 0.0.0.0 255.255.0.0 U 0 0 0 vlan1
0.0.0.0 10.112.112.113 0.0.0.0 UG 0 0 0 ppp1
Route IP Netmask Router Interface Metri
Kernel 192.168.1.3 255.255.0.0 192.168.1.1 WIFI and LAN Ethernet ports 1
Quagga 192.168.144.29 255.255.0.0 192.168.144.17 WIFI and LAN Ethernet ports 2
Kernel 10.10.10.2 255.255.0.0 10.10.10.4 WAN Ethernet port 1
Quagga 255.255.0.0 0.0.0.0 0.0.0.0 WIFI and LAN Ethernet ports 1
Quagga 10.112.112.3 10.112.112.113 0.0.0.0 PPPoE interface 0
Kernel 0.0.0.0 0.0.0.0 0.0.0.0 PPP interface 1
Kernel 0.0.0.0 0.0.0.0 0.0.0.0 GRE tunnel 1 0
Quagga 0.0.0.0 0.0.0.0 0.0.0.0 GRE tunnel 0 0
Disabled 0.0.0.0 0.0.0.0 0.0.0.0 WIFI and LAN Ethernet ports 0
Disabled 0.0.0.0 0.0.0.0 0.0.0.0 WIFI and LAN Ethernet ports 0
Save

Note that the Static Routes configuration screen has two distinct parts:

- the **upper** pane **displays** the current routing table, such as:



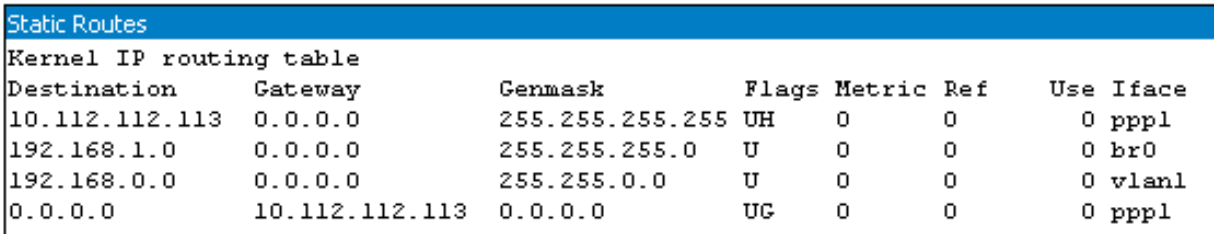
Kernel IP routing table

Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
192.168.1.148	0.0.0.0	255.255.255.255	UH	0	0	0	br0
10.112.112.112	0.0.0.0	255.255.255.255	UH	0	0	0	ppp0
10.0.0.0	0.0.0.0	255.255.255.0	U	0	0	0	vlan1
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	br0
10.0.2.0	0.0.0.0	255.255.255.0	U	0	0	0	gretun0
0.0.0.0	10.112.112.112	0.0.0.0	UG	0	0	0	ppp0

Here you can only see the existing static routes for BYTTON (default routes, gateway, masquerading if used, interface used, and so on), you cannot perform changes;

- the **lower** pane allows you to **define** up to ten (10) static routes:

Static Route Display



Static Routes

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
10.112.112.113	0.0.0.0	255.255.255.255	UH	0	0	0	ppp1
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	br0
192.168.0.0	0.0.0.0	255.255.0.0	U	0	0	0	vlan1
0.0.0.0	10.112.112.113	0.0.0.0	UG	0	0	0	ppp1

The routes are shown top downwards from the most specific to the least specific.

Destination - the destination network or host system. Declaring a default route means adding a route with 0.0.0.0 as its destination.

Gateway - the access gateway the respective routing entry points to. If this field has only zeroes (0.0.0.0) or an asterisk (*), this means no gateway is used, the destination network is connected directly to the computer.

Genmask - the bit mask applied to the destination. It shows the "generality" of the route.

Flags - indicator flags that describe some characteristics of the route. Such flags are:

U - the route is active and operating, the interface to be used is up;

G - the route uses an external gateway (the network interfaces of the system supply routes to the networks which are directly connected, all other routes use external gateways. Thus, the networks which are directly connected don't have the G flag, but it is activated for all other routes).

H – it is a route towards a single host instead of a network.

D - the table entry has been generated dynamically, either by a routing protocol or by a an ICMP redirect message (see section 3.5).

M – this route was modified by a dynamic routing protocol;

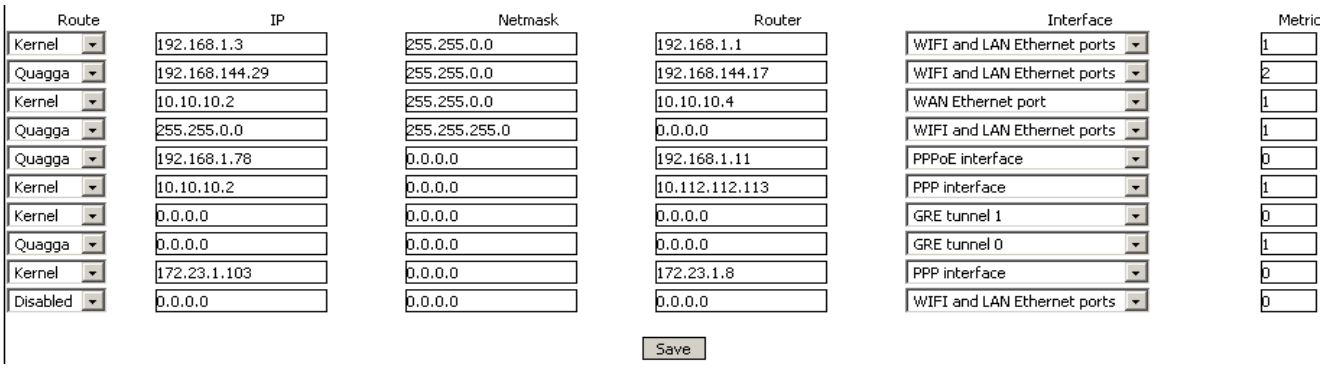
R - the route vas re-activated following update by dynamic routing protocol. Routes may be configured as passive or static even when a protocol for dynamic routing is used.

Other fields refer to the **Metric** (routing cost), the number of references to this route, etc,

Finally, **Iface** is the name of the network interface used for this route.

Static Route Definition

Such a static route is a possible path from a device to its destination or to another host. This way the Bytton router will be able to know where it may deliver the data packets coming from the Internet with different destination IP addresses.


Route
IP
Netmask
Router
Interface
Metric
Kernel 192.168.1.3 255.255.0.0 192.168.1.1 WIFI and LAN Ethernet ports 1
Quagga 192.168.144.29 255.255.0.0 192.168.144.17 WIFI and LAN Ethernet ports 2
Kernel 10.10.10.2 255.255.0.0 10.10.10.4 WAN Ethernet port 1
Quagga 255.255.0.0 255.255.255.0 0.0.0.0 WIFI and LAN Ethernet ports 1
Quagga 192.168.1.78 0.0.0.0 192.168.1.11 PPPoE interface 0
Kernel 10.10.10.2 0.0.0.0 10.112.112.113 PPP interface 1
Kernel 0.0.0.0 0.0.0.0 0.0.0.0 GRE tunnel 1 0
Quagga 0.0.0.0 0.0.0.0 0.0.0.0 GRE tunnel 0 1
Kernel 172.23.1.103 0.0.0.0 172.23.1.8 PPP interface 0
Disabled 0.0.0.0 0.0.0.0 0.0.0.0 WIFI and LAN Ethernet ports 0
Save

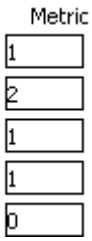
For each route you may perform these settings:

Route: Enable or Disable. By default, all ten are disabled.
Now the button of each route allows you to select who will perform the routing, either the Kernel or the Quagga routing program:

IP: Address of the remote network or host to which you want to assign a static route.
Netmask: the subnet mask determines which portion of the destination IP address is the network part and which is the host part
Router: the gateway to be used, enter here the IP address of the router which allows for contact between Bytton and the remote host or network.
Interface: the interface to be used for the respective route. You may select one of the following available options: local network (WIFI and LAN Ethernet ports), WAN Ethernet port, PPP interface (HSDPA modem), PPPoE (PPP link over the Ethernet), GRE Tunnel0 or GRE Tunnel1.

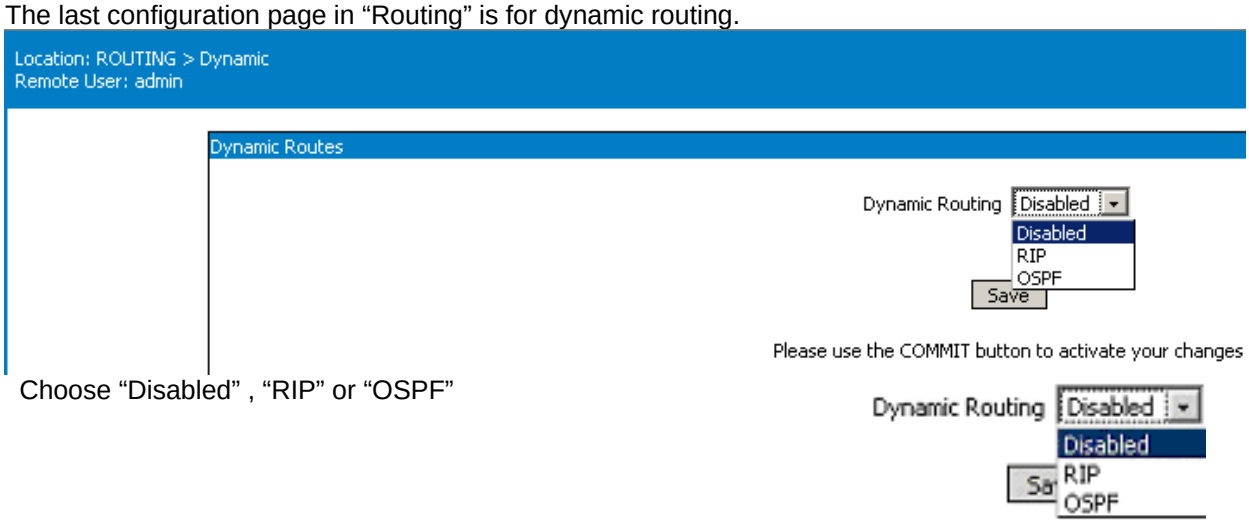
Metric:

Routing now features also the *metric* parameter: in case of multiple paths to the destination, you may specify the metric for each route (0, 1, and 2 etc).
The routing program will check the metric to select the shortest route for the data packets.



5.4.3 Dynamic routes

The last configuration page in "Routing" is for dynamic routing.



Choose "Disabled" , "RIP" or "OSPF"

In the Dynamic mode of routing, you need not specify fixed routes. Instead, the router adjusts automatically to physical changes in the layout of the network and it exchanges routing tables with other routers

Quagga routing

Quagga is a routing software suite for Unix platforms such as Linux, and it has been embedded into the BYTTON firmware. It provides implementations of DYNAMIC ROUTING PROTOCOLS

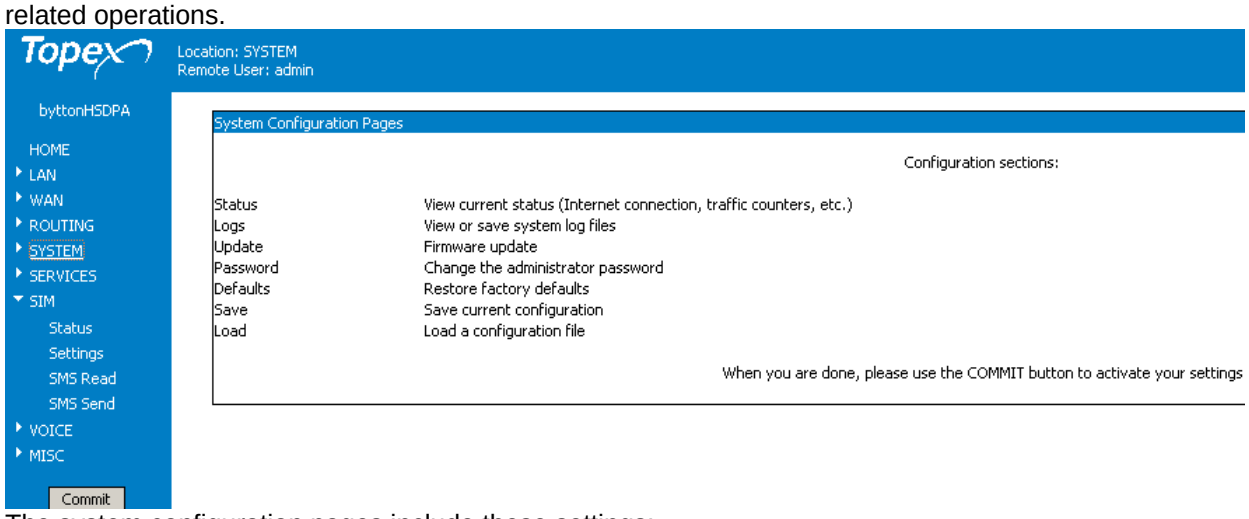
In order to configure dynamic routes with Quagga, the system administrator must connect to the programming console of BYTTON via SSH.

Currently implemented are ospf and rip,

Don't forget to click the Save button and then "Commit" to make permanent the change you performed!

5.5 SYSTEM

Shows the current state of the equipment and the logs, also allowing you to perform several system-related operations.

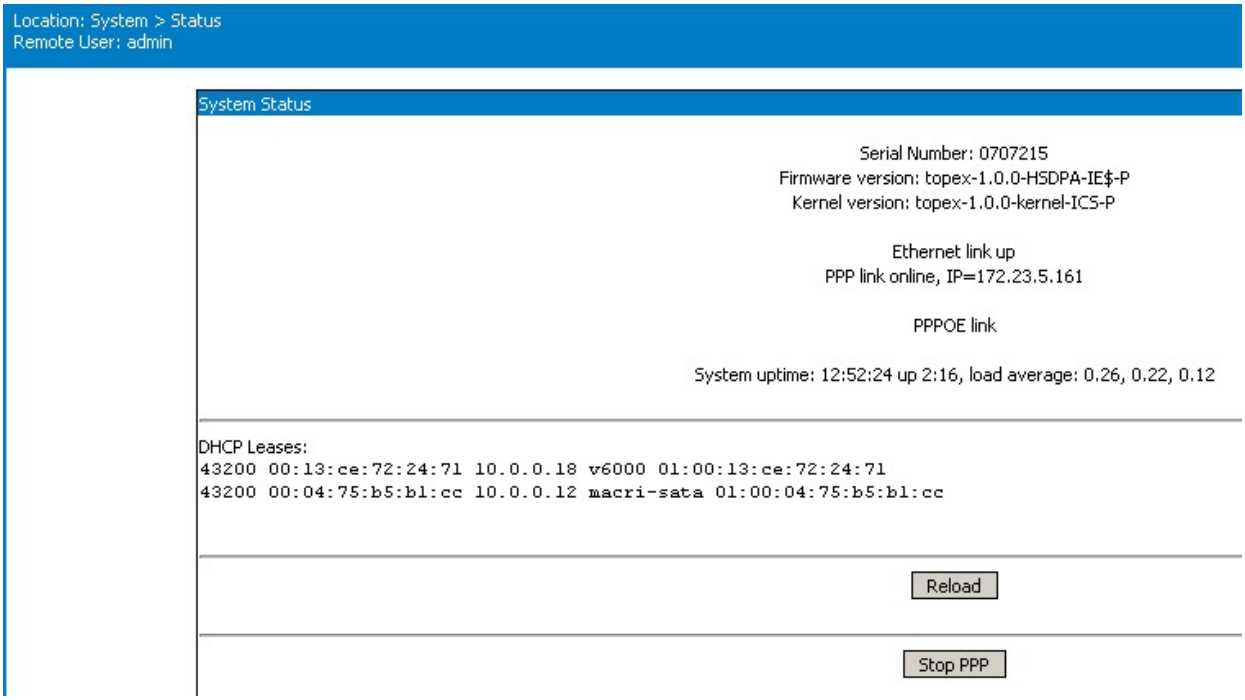


The system configuration pages include these settings:

- Status, displays the current status of the BYTTON HSDPA equipment
- Logs, shows the log file
- Update, you may perform firmware update
- Password, allows modification of the password
- Defaults, restores the factory default settings
- Save, saves the current configuration of BYTTON
- Load, loads a stored configuration.

5.5.1. Status

Shows the status of the BYTTON HSDPA system:



This page displays information about the following items:

- Serial Number: each Bytton HSDPA from Topex has an unique identification number, such as 0707214, 0707215, etc;
- Firmware version: version of the firmware running on BYTTON: you may see "Firmware version is 0.6.3" or "topex-1.2.3 –NETWORK-xyz-P" in the above example, and so on.
- Kernel version. Operaing system version.
- The frimware and operating system may be updated separately, according to the requirements of the users. The operating system memory is write-protected, thus in case of problems, accidental erasure or power failure during updating, you still have a functional "kernel" allowing you to load a new software image;
- state of the Ethernet link: up (active) or not:

- State of the Ethernet link, if used: up (active). When using ETH for the WAN connection, the PPP/PPPoE links will be inactive:	Firmware version is 0.6.3-HSDPA-P Ethernet link up PPP link offline
– State of the PPP data link, which uses the embedded modem of the Bytton equipment. It may be in one of these states: online (active), offline or stopped. Stopped means it is Disabled, while Offline may indicate temporary connection hang-up, but it activates when Bytton sends/recieves data traffic. If the PPP link is online, the IP allotted by your provider will also be shown. – AND – State of the PPPOE data link, which uses the WAN Ethernet port for the PPP connection.	PPP link online, IP=172.23.5.161 PPPOE link

System uptime: time since the last restart of the BYTTON equipment, both in full format (hours:minutes:seconds) and short format (up 1 minute)

- Load average: "0.06, 0.04, 0.01" - info about system loading (maximum value / average value / number of active processes)
- DHCP Leases: temporary assigned IP addresses and their coresponding MAC, host name, validity period, etc.

```
DHCP Leases:

946729927 00:13:ce:72:24:71 192.168.1.18 v6000 01:00:13:ce:72:24:71
946728682 00:04:75:b5:b1:cc 192.168.1.12 mcr-p4-w40 01:00:04:75:b5:b1:cc
```

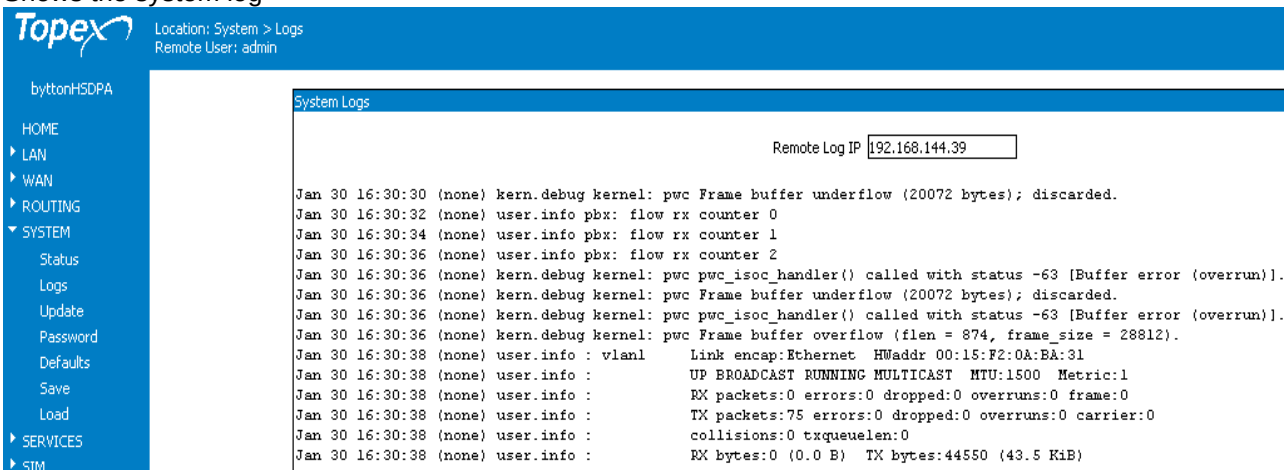
The "**Reload**" button at the bottom of the page refreshes BYTTON's status information.

The "**Please reload**!" message appears when the internal PPP link is in a transition state: "PPP link starting". Since the state is by definition temporary, you **must** click the Reload button in order to get the current status of the PPP link.

Start/Stop PPP
This new feature allows you to manually start and stop the PPP link. When PPP link status is online, the button will display "Stop", since it now allows you to stop the PPP link (break the connection). After you have stopped the PPP connection, the button changes to "Start PPP"

5.5.2. Logs

Shows the system log


Topex
Location: System > Logs
Remote User: admin
byttonHSDPA
HOME
LAN
WAN
ROUTING
SYSTEM
Status
Logs
Update
Password
Defaults
Save
Load
SERVICES
SIM
System Logs
Remote Log IP 192.168.144.39
Jan 30 16:30:30 (none) kern.debug kernel: pwc Frame buffer underflow (20072 bytes); discarded.
Jan 30 16:30:32 (none) user.info pbx: flow rx counter 0
Jan 30 16:30:34 (none) user.info pbx: flow rx counter 1
Jan 30 16:30:36 (none) user.info pbx: flow rx counter 2
Jan 30 16:30:36 (none) kern.debug kernel: pwc pwc_isoc_handler() called with status -63 [Buffer error (overrun)].
Jan 30 16:30:36 (none) kern.debug kernel: pwc Frame buffer underflow (20072 bytes); discarded.
Jan 30 16:30:36 (none) kern.debug kernel: pwc pwc_isoc_handler() called with status -63 [Buffer error (overrun)].
Jan 30 16:30:36 (none) kern.debug kernel: pwc Frame buffer overflow (flen = 874, frame_size = 28812).
Jan 30 16:30:38 (none) user.info : vlan1 Link encap:Ethernet HWaddr 00:15:F2:0A:BA:31
Jan 30 16:30:38 (none) user.info : UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
Jan 30 16:30:38 (none) user.info : RX packets:0 errors:0 dropped:0 overruns:0 frame:0
Jan 30 16:30:38 (none) user.info : TX packets:75 errors:0 dropped:0 overruns:0 carrier:0
Jan 30 16:30:38 (none) user.info : collisions:0 txqueuelen:0
Jan 30 16:30:38 (none) user.info : RX bytes:0 (0.0 B) TX bytes:44550 (43.5 KiB)

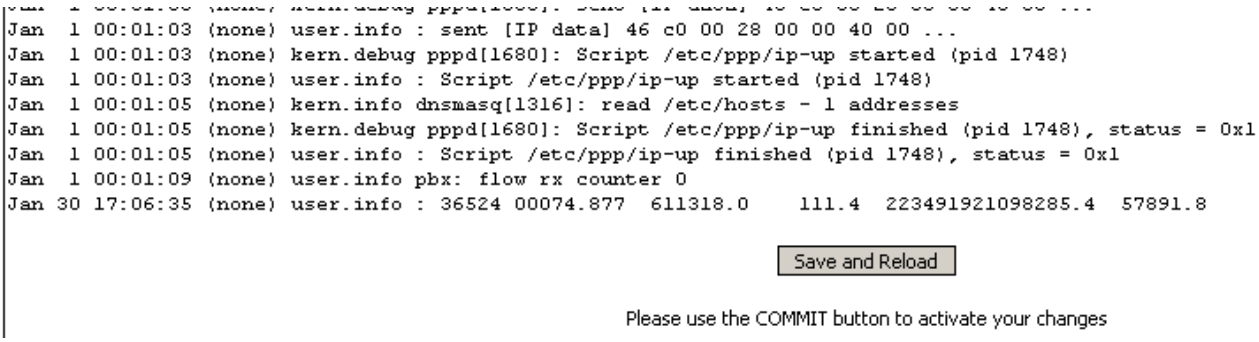
The log is a place where all the applications running on the BYTTON equipment store their output messages: status reports, confirmation or error messages, activity, and so on. It is a plain text (thus easy to interpret) record of actions taken by the software as it runs on Bytton: changes made, devices and drivers detected, files added or deleted, communication with the modem, network settings, and so on.
Correspondingly, in the log you will see records of the kernel or of the user, debug messages, info or warnings:

```
Mar 14 09:06:36 (none) user.info pbx: modem err port open
Mar 14 09:06:36 (none) user.info : PING 193.226.173.50 (193.226.173.50): 56 data bytes
Mar 14 09:06:36 (none) user.info : 64 bytes from 193.226.173.50: icmp_seq=0 ttl=55 time=2696.6 ms
Mar 14 09:06:36 (none) user.info : 64 bytes from 193.226.173.50: icmp_seq=2 ttl=55 time=1827.7 ms
Mar 14 09:06:36 (none) user.info : --- 193.226.173.50 ping statistics ---
Mar 14 09:06:36 (none) user.info : 3 packets transmitted, 2 packets received, 33% packet loss
Mar 14 09:06:36 (none) user.info : round-trip min/avg/max = 1827.7/2262.1/2696.6 ms
```

The log is very helpful when troubleshooting. It may be saved on your PC (simply use "Save As" option of your browser) for further examination.

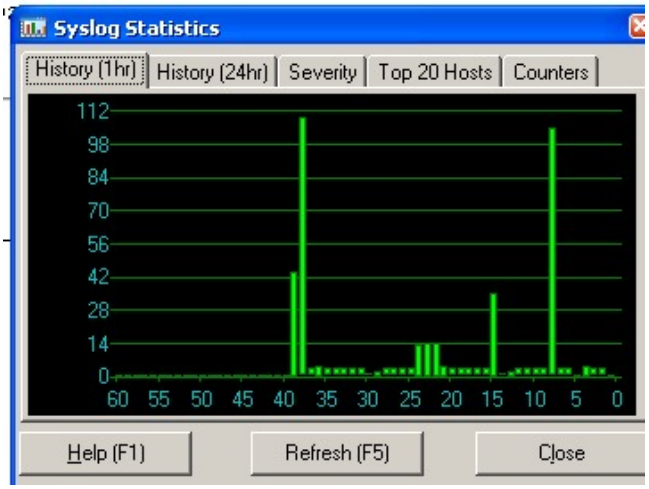
Remote Log IP: address where the log will be sent upon occurrence of events. Use this IP setting to send the log messages to a remote location. If you leave this address "0.0.0.0" it means the log won't be sent.

Note: The remote machine must run a Syslog client, such as the "syslogd" daemon under Linux or a corresponding syslog client application for Windows.

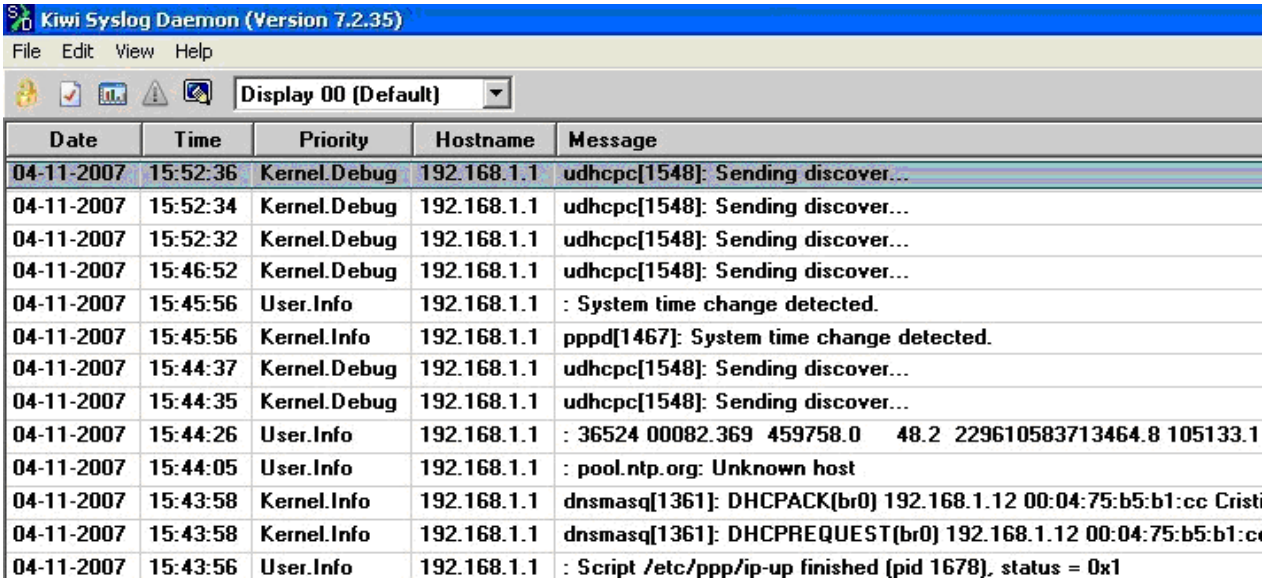

Jan 1 00:01:03 (none) user.info : sent [IP data] 46 c0 00 28 00 00 40 00 ...
Jan 1 00:01:03 (none) kern.debug pppd[1680]: Script /etc/ppp/ip-up started (pid 1748)
Jan 1 00:01:03 (none) user.info : Script /etc/ppp/ip-up started (pid 1748)
Jan 1 00:01:05 (none) kern.info dnsmasq[1316]: read /etc/hosts - 1 addresses
Jan 1 00:01:05 (none) kern.debug pppd[1680]: Script /etc/ppp/ip-up finished (pid 1748), status = 0x1
Jan 1 00:01:05 (none) user.info : Script /etc/ppp/ip-up finished (pid 1748), status = 0x1
Jan 1 00:01:09 (none) user.info pbx: flow rx counter 0
Jan 30 17:06:35 (none) user.info : 36524 00074.877 611318.0 111.4 223491921098285.4 57891.8
Save and Reload
Please use the COMMIT button to activate your changes

To update the Log, press the "Save and Reload" button located at the bottom of the screen.

An example of a free Syslog Daemon program for Windows is **Kiwi** , from Kiwi Enterprises:



See below an extract form the screen of the Kiwi program, which runs on the destination PC and receives the Syslog sent out by Bytton HSDPA device:


Kiwi Syslog Daemon (Version 7.2.35)
File Edit View Help
Display 00 (Default)
Date Time Priority Hostname Message
04-11-2007 15:52:36 Kernel.Debug 192.168.1.1 udhcpc[1548]: Sending discover...
04-11-2007 15:52:34 Kernel.Debug 192.168.1.1 udhcpc[1548]: Sending discover...
04-11-2007 15:52:32 Kernel.Debug 192.168.1.1 udhcpc[1548]: Sending discover...
04-11-2007 15:46:52 Kernel.Debug 192.168.1.1 udhcpc[1548]: Sending discover...
04-11-2007 15:45:56 User.Info 192.168.1.1 : System time change detected.
04-11-2007 15:45:56 Kernel.Info 192.168.1.1 pppd[1467]: System time change detected.
04-11-2007 15:44:37 Kernel.Debug 192.168.1.1 udhcpc[1548]: Sending discover...
04-11-2007 15:44:35 Kernel.Debug 192.168.1.1 udhcpc[1548]: Sending discover...
04-11-2007 15:44:26 User.Info 192.168.1.1 : 36524 00082.369 459758.0 48.2 229610583713464.8 105133.1
04-11-2007 15:44:05 User.Info 192.168.1.1 : pool.ntp.org: Unknown host
04-11-2007 15:43:58 Kernel.Info 192.168.1.1 dnsmasq[1361]: DHCPACK(br0) 192.168.1.12 00:04:75:b5:b1:cc Cristi
04-11-2007 15:43:58 Kernel.Info 192.168.1.1 dnsmasq[1361]: DHCPREQUEST(br0) 192.168.1.12 00:04:75:b5:b1:c
04-11-2007 15:43:56 User.Info 192.168.1.1 : Script /etc/ppp/ip-up finished (pid 1678), status = 0x1

Setting the level of details in the system log

In the configuration page "VOICE>Settings" there is a field that establishes how detailed will be the debug messages stored in the Log.

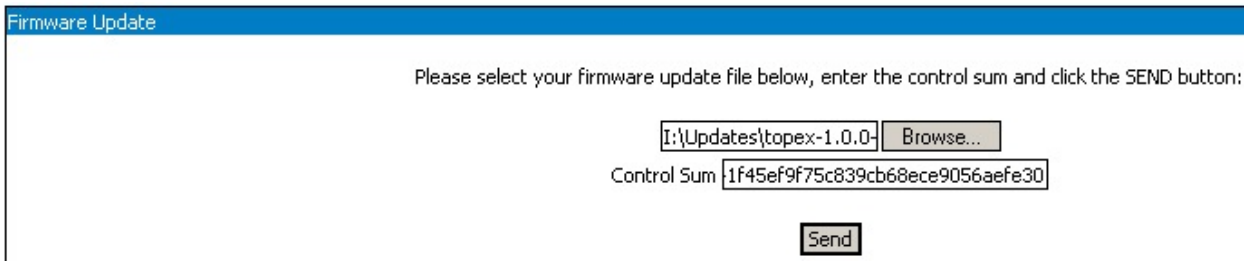
These messages are for troubleshooting purpose only, they are of no interest in everyday use.

The default is "000", recording the least number of messages.
If you set Debug Messages to "111", in System Log will be recorded all the debug messages, generating something like this:

```
Jan  1 00:09:30 (none) kern.debug udhcpc[1397]: Sending discover...
Jan  1 00:09:31 (none) user.info pbx: modem rcv \0d\0a^DSFLOWRPT:000001F2,00000000,00000000,00000000000003EFE,0000000000006028,
Jan  1 00:09:31 (none) user.info pbx: flow rx counter 17
Jan  1 00:09:32 (none) user.info pbx: modem rcv \0d\0a^BOOT:438774,0,0,0,9\0d\0a
Jan  1 00:09:33 (none) user.info pbx: modem rcv \0d\0a^DSFLOWRPT:000001F4,00000000,00000000,00000000000003EFE,0000000000006028,
Jan  1 00:09:33 (none) user.info pbx: flow rx counter 18
Jan  1 00:09:35 (none) user.info pbx: modem snd AT+CREG?\0d
Jan  1 00:09:35 (none) user.info pbx: modem rcv AT+CREG?\0d\0d\0a+CREG: 0,1\0d\0a\0d\0a0K\0d\0a
Jan  1 00:09:35 (none) user.info pbx: modem rcv \0d\0a^DSFLOWRPT:000001F6,0000006B,0000003C,00000000000003FD4,00000000000060A0,
Jan  1 00:09:37 (none) user.info pbx: modem rcv \0d\0a^DSFLOWRPT:000001F8,00000074,0000009C,00000000000040BD,00000000000061D8,
Jan  1 00:09:39 (none) user.info pbx: modem rcv \0d\0a^DSFLOWRPT:000001FA,00000028,00000028,000000000000410D,0000000000006228,
Jan  1 00:09:41 (none) user.info pbx: modem rcv \0d\0a^DSFLOWRPT:000001FC,00000000,00000000,000000000000410D,0000000000006228,
Jan  1 00:09:41 (none) user.info pbx: flow rx counter 0
Jan  1 00:09:43 (none) user.info pbx: modem rcv \0d\0a^DSFLOWRPT:000001FE,00000000,00000000,000000000000410D,0000000000006228,
Jan  1 00:09:43 (none) user.info pbx: flow rx counter 1
Jan  1 00:09:45 (none) user.info pbx: modem snd AT+CREG?\0d
Jan  1 00:09:45 (none) user.info pbx: modem rcv AT+CREG?\0d\0d\0a+CREG: 0,1\0d\0a\0d\0a0K\0d\0a
Jan  1 00:09:45 (none) user.info pbx: modem rcv \0d\0a^DSFLOWRPT:00000200,00000020,00000000,000000000000414D,0000000000006228,
Jan  1 00:09:45 (none) user.info pbx: flow rx counter 2
Jan  1 00:09:47 (none) user.info pbx: modem rcv \0d\0a^DSFLOWRPT:00000202,00000000,00000000,000000000000414D,0000000000006228,
Jan  1 00:09:47 (none) user.info pbx: flow rx counter 3
Jan  1 00:09:49 (none) user.info pbx: modem rcv \0d\0a^DSFLOWRPT:00000204,00000000,00000000,000000000000414D,0000000000006228,
Jan  1 00:09:49 (none) user.info pbx: flow rx counter 4
Jan  1 00:09:51 (none) user.info pbx: modem rcv \0d\0a^DSFLOWRPT:00000206,00000000,00000000,000000000000414D,0000000000006228,
Jan  1 00:09:51 (none) user.info pbx: flow rx counter 5
Jan  1 00:09:53 (none) user.info pbx: modem rcv \0d\0a^DSFLOWRPT:00000208,00000000,00000000,000000000000414D,0000000000006228,
Jan  1 00:09:53 (none) user.info pbx: flow rx counter 6
```

5.5.3. Update

Allows you to perform an update or upgrade of the firmware running on BYTTON HSDPA.

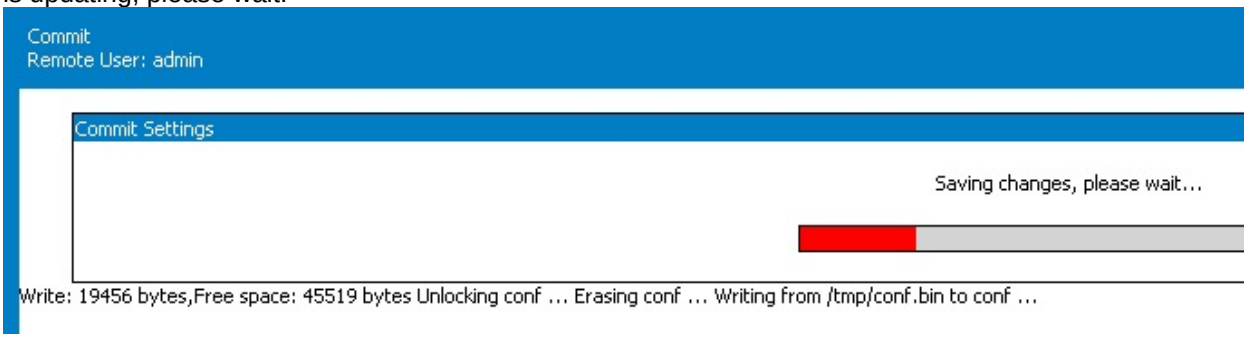


The update (firmware image) must be on your PC. The image files have the extension "trx"
You may download the image files from the TOPEX website. The update files are called "topex-1.2.3-HSDPA-x.y.z-P.trx", where 1.2.3. is the version number, for instance 0.6.0. or 1.0.1

Enter the name of the update or click Browse to search your system for it. Select the file you want and press Open.

Note:
*Each firmware file has an associated **Control Sum.** The control sum is a string of hexadecimal figures, such as "f2209c63972be34f55d4e69d90042d93" and it is stored in a text file (with .txt extension), with the same name as the firmware image. Using a control sum prevents you from loading a corrupted image. The Control Sum is located in a txt with the same name as the firmware. Copy the Control Sum from this file and paste it in the web-page in the field named "Control Sum"*

Now click the "Send" button to perform the update.
A "Firmware Update" window shows up, you can see a progress indicator under the message "Firmware is updating, please wait!"


Commit
Remote User: admin
Commit Settings
Saving changes, please wait...
Write: 19456 bytes,Free space: 45519 bytes Unlocking conf ... Erasing conf ... Writing from /tmp/conf.bin to conf ...

Note that there are **two** distinct, successive phases of updating the firmware image:

- in the first one, while the message "Updating firmware" is blinking, the equipment just checks the program image to be loaded against its checksum.
- if the result is OK, the BYTTON device goes to the second phase, it really loads the new firmware into its Flash memory. In this phase, the progress indicator is colored in red and additional messages are show: Write: … bytes, Free space: … bytes, Unlocking …, Erasing …, Writing to …

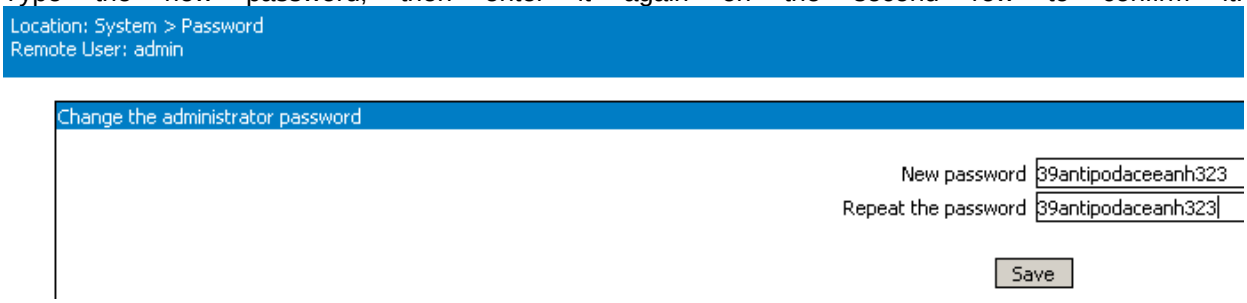
Warning! *Do not update the firmware unless you have problems with the Bytton router or the new firmware has a feature that you need. Remember to backup your current configuration first. Be careful when you load an update file. If you select a wrong file, or if for different reasons firmware upgrading fails, the equipment may no longer operate correctly. You will need to perform an update using the "kernel" mode.*

To avoid this, follow carefully the rules indicated here.

- don't turn off the BYTTON equipment or the computer while the firmware is being overwritten
- equipment does not work while firmware update is in progress.
- after successful updating, verify the upgraded firmware
- remember that updating the firmware on the BYTTON HSDPA equipment could cause some or all of the configuration settings to be lost, depending on the degree of change in the firmware. Therefore it is highly recommended that you **save** your current configuration before updating, then you restore it. To backup your settings, perform a Save, update the firmware, and then Load the saved settings, after you have the equipment operating with the updated firmware.

5.5.4. Password

Allows you to modify passwords for the two log-in accounts: "admin" and "user". For changing the "admin" account password you must be logged in as admin , and for changing/modifying the "user" account password you must be logged in as "user".
From here-on the procedure is the same.
Type the new password, then enter it again on the second row to confirm it.



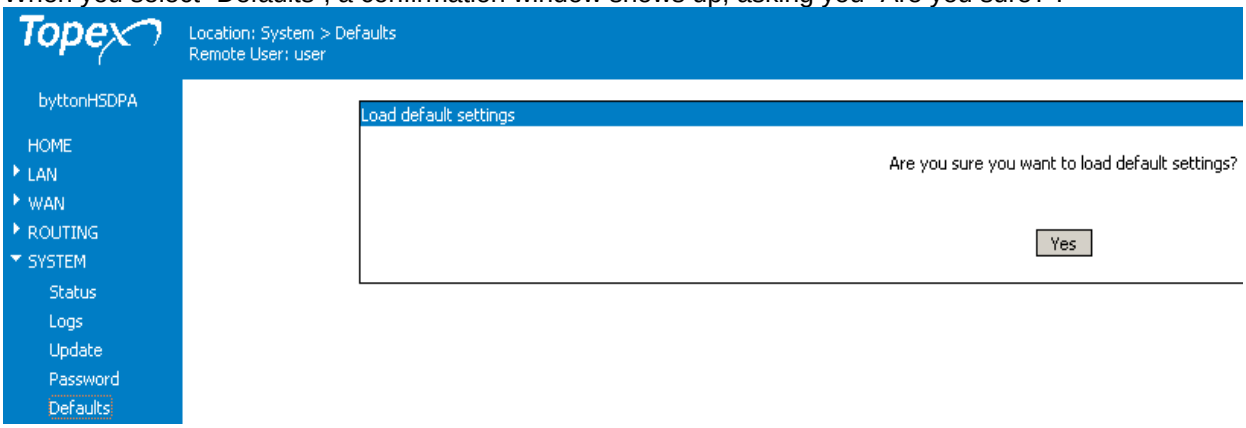
"Save" saves the new password.
You should replace the default password (99admin11) with one of your own as soon as possible.

Please choose a password with **minimum** six characters. In order to effectively prevent unauthorized access, the password must be long enough and include both letters and numbers.
Note that the password is **case-sensitive**.

Remember that you must change both passwords, the one for "user" and respectively the one for "admin".
The example above has shown the modification of the admin password, you should proceed in the same way to perform change of the password for "user", following a successful log-in as "user".

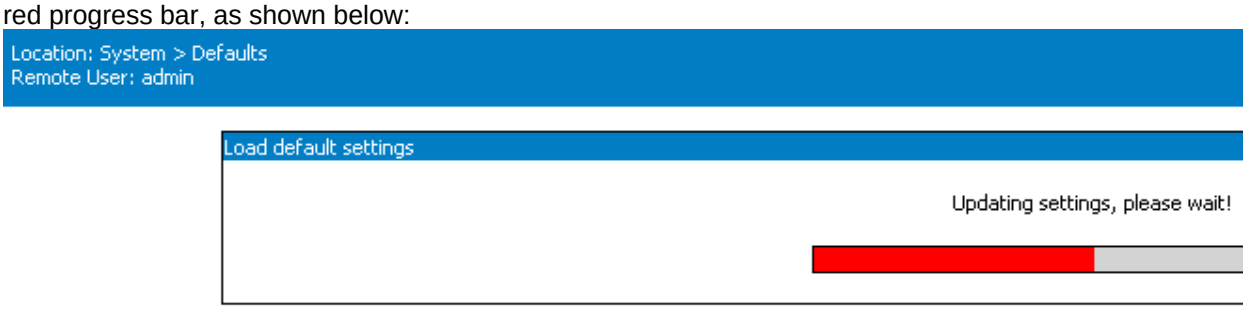
5.5.5. Defaults

This option restores the system settings to factory defaults.
When you select "Defaults", a confirmation window shows up, asking you "Are you sure?".



If you want to proceed, click the YES button and the equipment will revert to the factory default settings. Following a reset, it will start operating with the factory default values for all parameters.

During the process you will see on screen the blinking message "Updating settings, please wait!" and a red progress bar, as shown below:



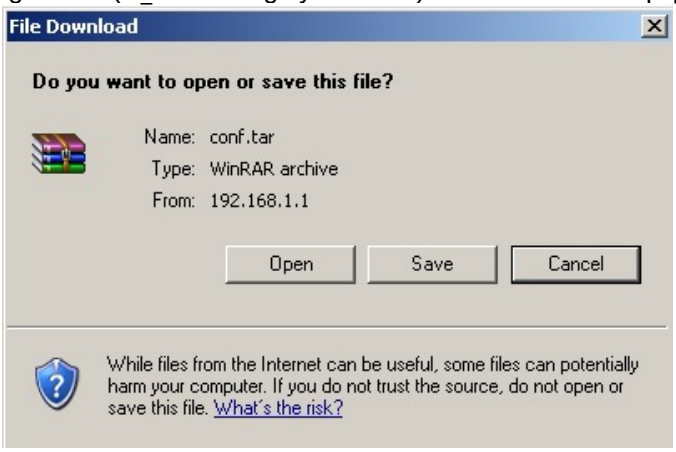
CAUTION!
Use this option carefully.
During the process, BYTTON will not be available for routing and connecting to the 3G network. For a few moments, the LAN icon in the status bar will be barred with a red "x" and the message "A network cable is unplugged" will show up, indicating that Bytton HSDPA is unavailable.

Hardware factory defaults
If you want, you can also perform the "Return to Defaults" operation via **hardware**.
This means you do not need to use the Web interface!
For this, simply press the **Reset** button (located on the back panel, among the connectors) for at least three seconds.
The BYTTON HSDPA equipment will reboot and revert to the factory default settings.
This way of restoring the factory default settings is faster than using the web interface, but you should exercise the same care.

5.5.6 Save

Makes a backup copy of the current configuration (all the settings you made) of the BYTTON equipment.

The configuration file is called by default "CONF.tar"
You will see a message similar to the one shown in this image


File Download
Do you want to open or save this file?
Name: conf.tar
Type: WinRAR archive
From: 192.168.1.1
Open
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

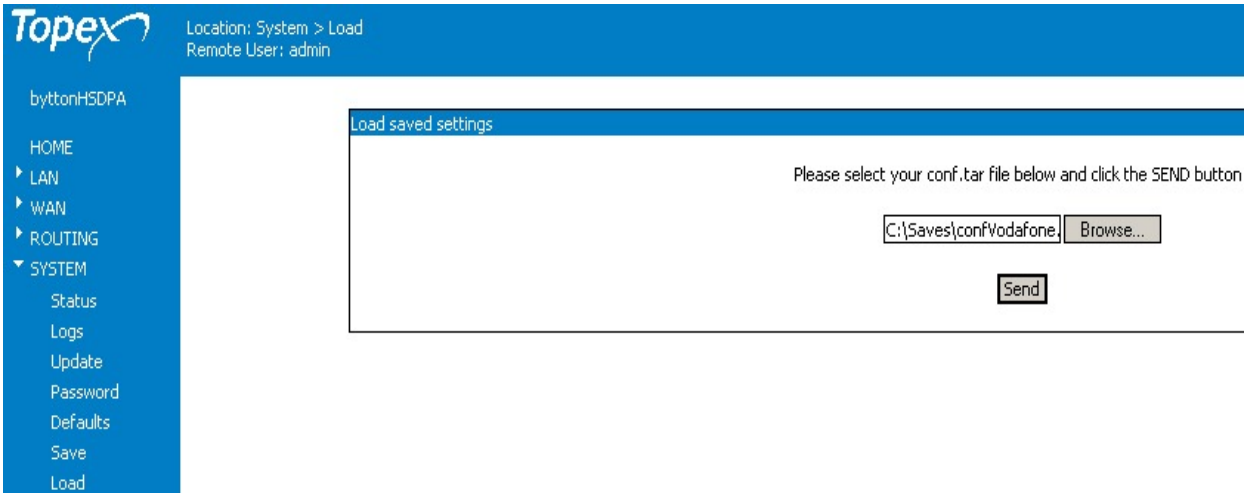
Click "Save" or select "Save it to disk" to save the file with the current configuration of BYTTON HSDPA.

You may select the folder where the configuration will be saved; also, you should change the default name "conf.tar" into a name meaningful for your actual configuration.

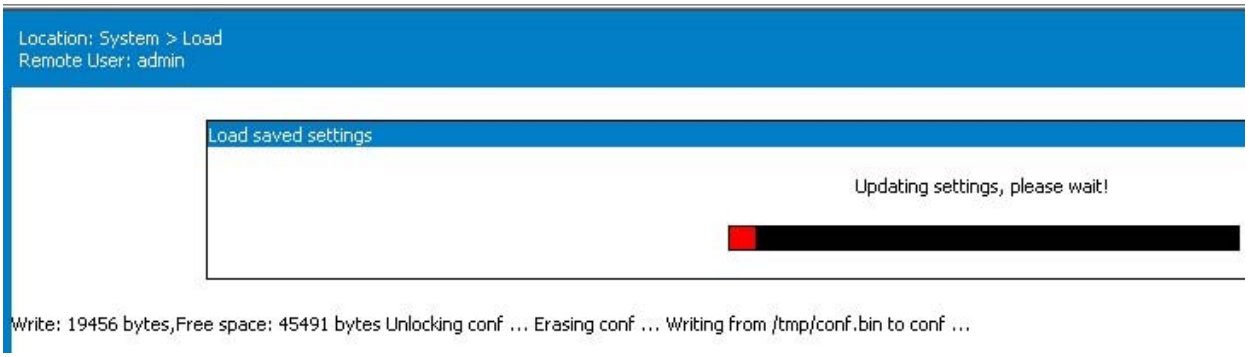
Note: *It is highly recommended that you backup your configuration from time to time. This way you can always load the saved configuration, if there is need. For instance, when you perform a "Restore to factory defaults", all previous settings are lost. If you have saved the configuration, you can load it back to perform changes.*
Also, you should perform a "Save" before using "Update" to load a new software image, since the new firmware could erase some of the settings.

5.5.7. Load

Loads a configuration file that has been previously saved or restores a backup.

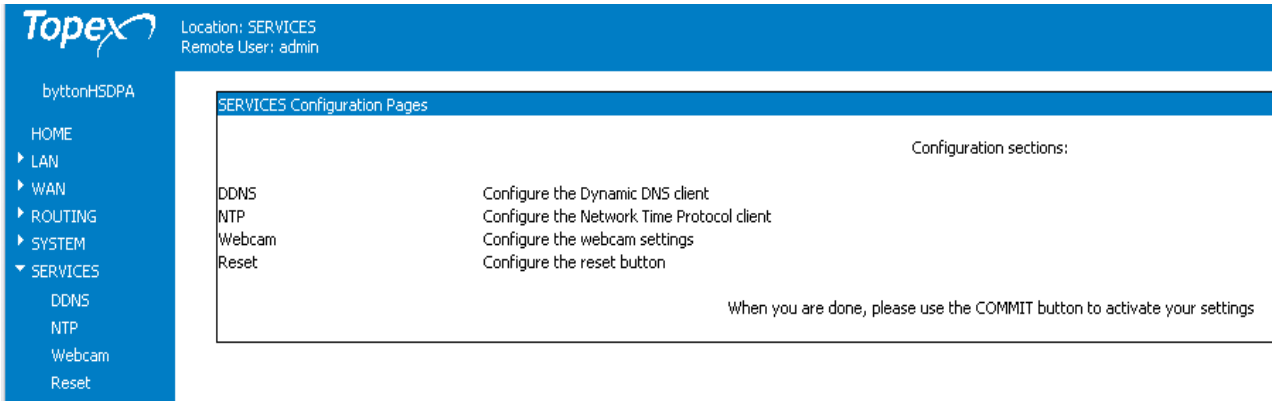


Use "Browse" to navigate to the location where you saved the configuration file. Press Open, then click "Send" to send the file to the BYTTON HSDPA equipment. A red progress bar will be displayed, and above it you will see the blinking message "Updating settings, please wait"


Location: System > Load
Remote User: admin
Load saved settings
Updating settings, please wait!
Write: 19456 bytes,Free space: 45491 bytes Unlocking conf ... Erasing conf ... Writing from /tmp/conf.bin to conf ...

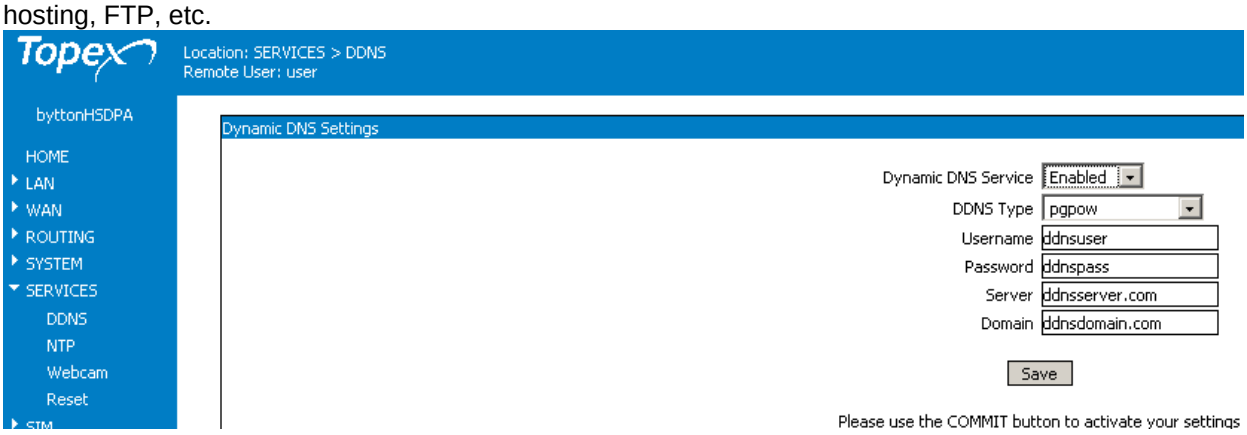
5.6 SERVICES

Here you may configure settings for the "services" provided by BYTTON, such as DDNS, NTP, webcam, and function of the RST button.

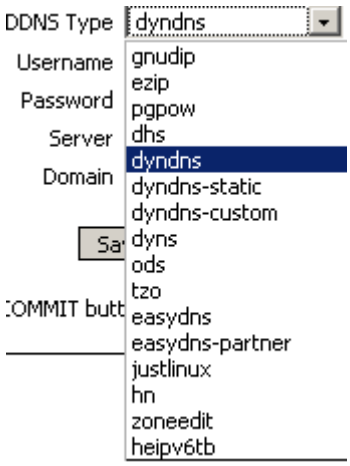


5.6.1 DDNS

Settings for the Dynamic DNS Server.
Dynamic DNS is a service that enables mapping of a dynamically assigned IP address to a static or permanent hostname. This allows the use of applications that require a static IP address, such as web-hosting, FTP, etc.



Dynamic DNS Service: Enables or disables the DDNS service.
This service allows you to export several hostnames by means of a Dynamic DNS provider.



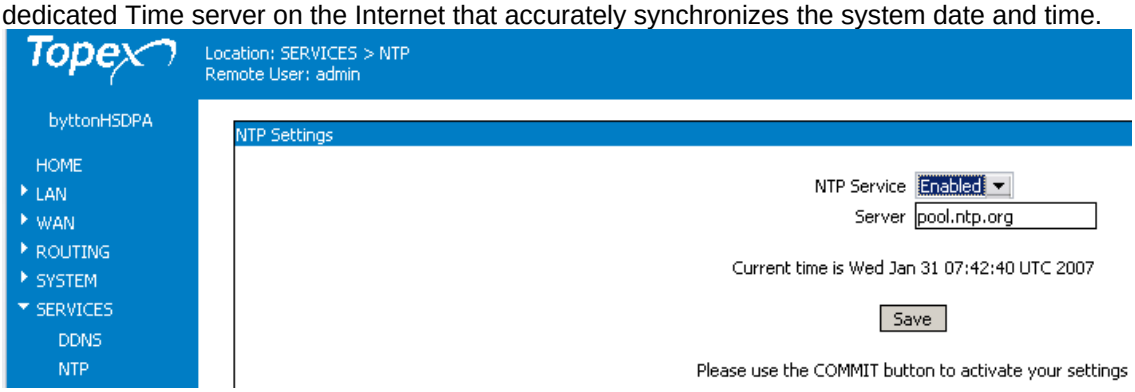
DDNS Type:
Allows you to select the type of DDNS service. The drop-down list includes the major Dynamic DNS service providers.
The default is gnudip.

Username & Password: User name and password for authenticating to the DDNS.
Server: Full name of the Dynamic DNS server used to store your host and domain name information.
Domain: The domain name for DDNS. You must have membership to one of the DDNS services providers.

Warning: *These factory default settings may not work in your area, you should change the DDNS parameters according to the specifications of your Internet provider.*

5.6.2 NTP

The **N**etwork **T**ime **P**rotocol is used to update the real-time clock in a computer, over Internet. It uses a dedicated Time server on the Internet that accurately synchronizes the system date and time.

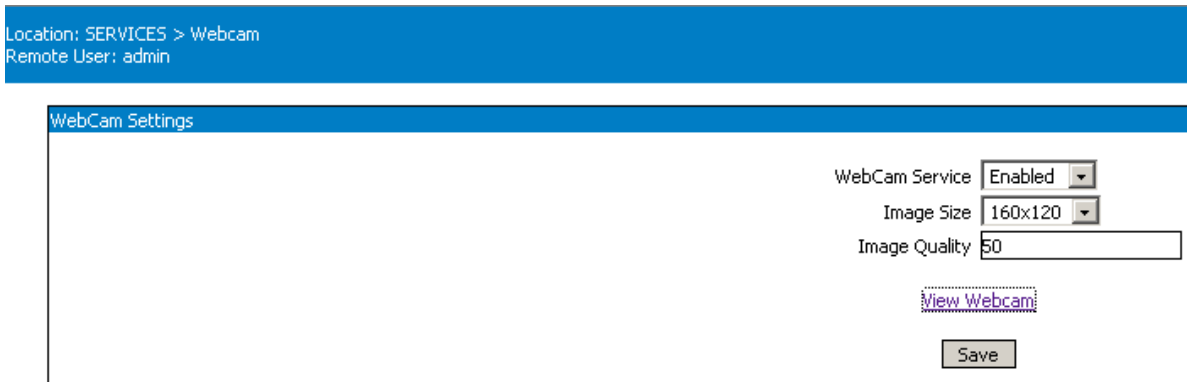


NTP Service: Enabled or Disabled
Server: enter the full name of the NTP server you want to use, such as "utcnist.colorado.edu" or "ro.pool.ntp.org".
The "Current time" indicator shows the current UTC time (Universal Coordinated Time) of the system, with millisecond precision.
If NTP server is not active, it will display the default UTC time, which is Jan 1, 2000.

This UTC time may be different from the local time of your computer!

5.6.3 Webcam

Shows and modifies settings of the web camera connected to BYTTON HSDPA.



WebCam Service: Enabled or Disabled.
Image Size: you may select one of the three values: 160x120, 320x240 or 640x480 (VGA). Default value is 320x240. It is recommended that you start with the **minimum** value, then increase it if it works, because some types of webcams do not support higher resolutions.
Image quality: Range is from 100 to zero, 100 being uncompressed and 0 maximum compression. Default value is 50, which gives a high compression and an acceptable quality and speed. Uncompressed images have the highest quality, but the resulting video file is large and the frame rate will be low.

Note: *Depending on the webcam model, you may have access to various controls. Usually, the live video screen inserted to the left.*

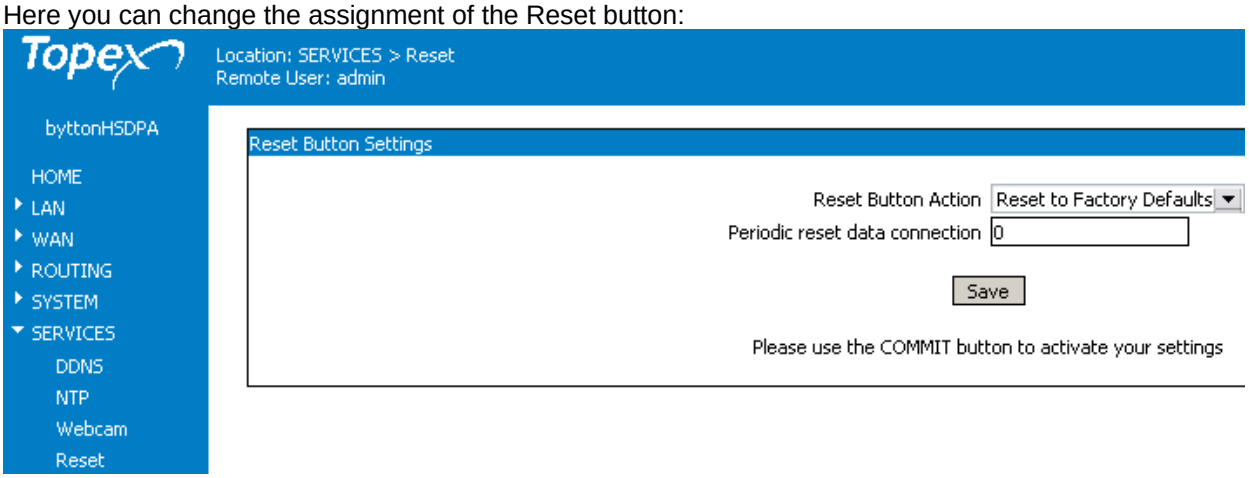
5.6.5 PWC compatible cameras

BYTTON's firmware direct operation (no additional software is needed) of webcams that are compatible with Linux PWC drivers. Decompression is supported for resolutions up to 640x480(maximum physical resolution of most CCD sensors)
There are limits to the maximum resolution and frame rate. Thus, VGA resolutions are limited to 15 fps because of the bandwidth available on the USB bus. The same cameras may work faster (up to 60 frames per second) when used at lower resolutions).
Other cameras only operate at quarter VGA resolutions: QCIF (176x144) or QSIF (160x120).
The PWC driver supports a wide range of general purpose webcams, such as:

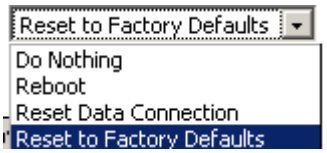
- from Philips: PCA645V,C PCA646VC, PCVC675K "Vesta" PCVC680K "Vesta Pro" PCVC690K "Vesta Scan", PCVC720K/40 "ToUCam XS", PCVC730K "ToUCam Fun", PCVC740K "ToUCam Pro", PCVC750K "ToUCam Scan" , PCVC830K "ToUCam Fun II", and PCVC840K "ToUCam Pro II";
- from Logitech: QuickCam 3000 Pro and 4000 Pro, QuickCam Notebook Pro, QuickCam Zoom, QuickCam Orbit/Sphere;
- from Creative Labs: old Webcam 5, Webcam Pro Ex;
- from Samsung: MPC-C10 and MPC-C30;
- from Visionite: VCS UM100, VCS UC300;
- SPC900NC;
- Sotec Afina Eye;
- Askey VC010 .

5.6.5. Reset

Here you can change the assignment of the Reset button:



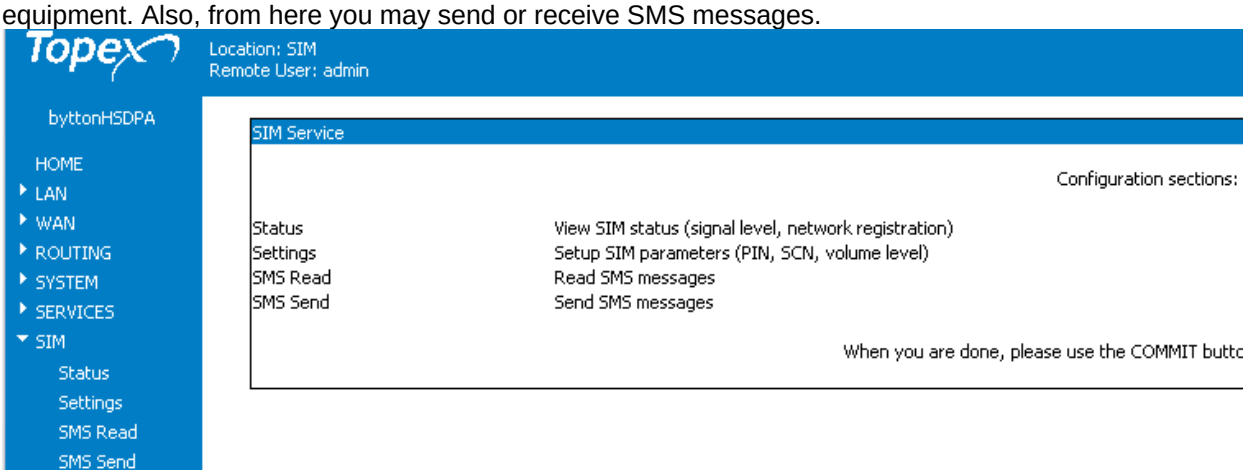
Reset Button Settings – you choose the option you want. The function of the Reset (RST) button, located on the back panel among the connectors, can be changed according to your needs.



Do nothing – yes, this "do nothing" action may quite be useful. It may happen that the Reset button is touched by accident when you plug a cable into Bytton HSDPA, so BYTTON reboots and reverts to the factory default values, loosing your particular settings. If you want to avoid this, select "Do nothing". Now, even if you accidentally press Reset, nothing happens. If you want, you can still perform Reset via software!
Reboot – it performs a full reboot (restart) of BYTTON HSDPA.
Reset Data Connection – only the data connection is resetted, the equipment does not stop operating.
Reset to Factory Defaults – after full reboot, BYTTON settings are restored to factory defaults.
Periodic reset data connection: after the specified number of seconds, the data connection will reset. The default value is 0 (zero), which means that the connection will never be restarted.

5.7 SIM

Here are the configuration pages related not only to the SIM card but also to the mobile module of the equipment. Also, from here you may send or receive SMS messages.



5.7.1. SIM Status

This page shows you the current state of the SIM card and of the GSM/GPRS/EDGE/UMTS/ HSDPA module.

The status of the HSDPA modules is automatically read every five seconds. The following information items are displayed:

- **Security**: "Unlocked" or "OK" means the SIM is active."Locked by PIN" means the SIM card is asking the PIN code to perform unlock.

As an additional security measure, the SIM card is also provided with a PUK code, requested after three wrong PIN codes.

- **Modem Version**: read from the 3G module.
- **IMSI** (International Mobile Subscriber Identity), subscriber's identity (SIM card identity). This is a unique 15 digits code number that identifies a mobile subscriber to the network. If the BYTTON's HSDPA module detects an active SIM card, it will query (and display) the IMSI code. Since the IMSI code is related to the SIM, when you change the SIM card you will have another IMSI code.

- **IMEI** (International Mobile Equipment Identifier). 15-digit number that uniquely identifies an individual mobile wireless terminal device. While IMSI is specific to the subscriber (SIM card), IMEI in specific to the equipment (BYTTON HDSPA modem)

If the SIM card is missing, the SIM Status window will show "error" in the Security, IMSI, Signal Level, Network and Registration fields.
But you will still see the version of the 3G modem and the IMEI code, since they are equipment-dependent, and not related to the SIM card.

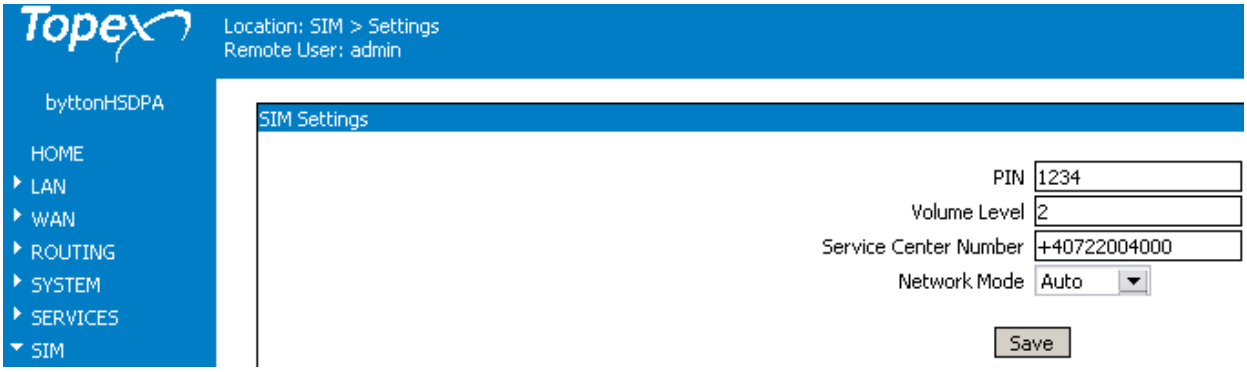
- **Signal Level**, displayed as two groups of two figures such as "15/30". The two digits indicate the level of the RF signal for the GSM/GPRS/EDGE/UMTS/HSDPA network on a scale from zero to 30. If the SIM card is missing or isn't registered,its status will be: "no signal".
- **Network**: the name of the mobile network which the equipment is registered to, as transmitted by the mobile carrier. It may also indicate the network type: 2G or 3G.

- **Registration status**: indicates whether the SIM card is registered to the mobile network or not.

Warning! *When the HSDPA module is in a call, or while it is transmitting or receiving SMS, it* ***cannot be interrogated about its state****.*
So if you click "SIM Status" while in a voice call, you will get an error message (ERR).
This does not mean something is wrong, simply try again (click "Reload") later, when you have finished the voice call or the transmission of SMS messages.

5.7.2. SIM Settings

In this section you may perform several settings related to the HSDPA module and to the SIM card.

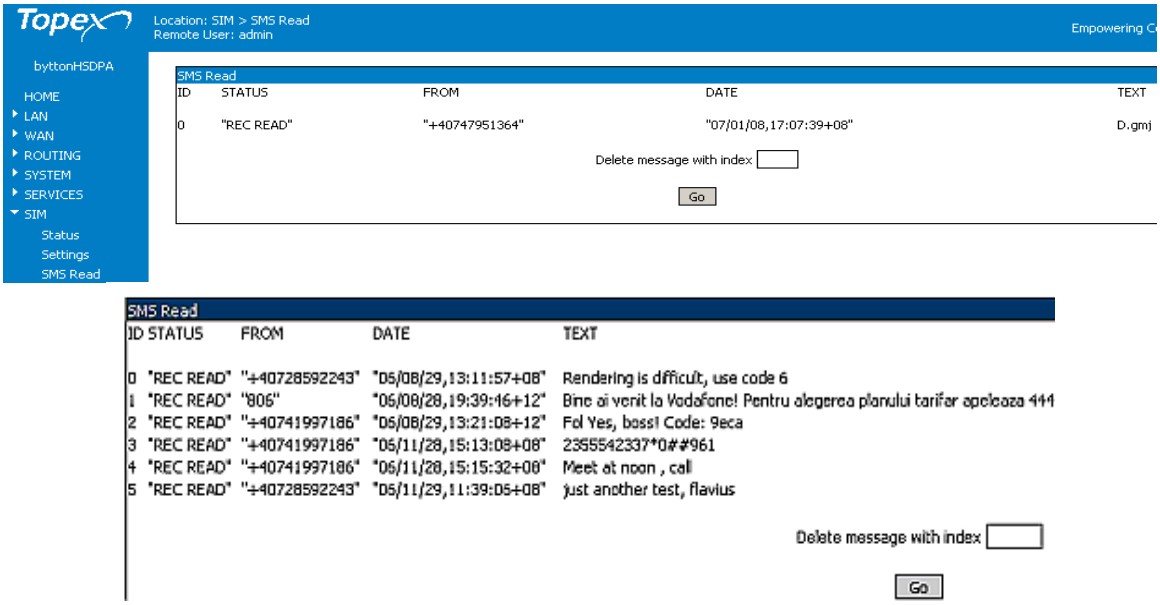


PIN: enter PIN code for the SIM card
Volume level: for setting the volume (sound) level.
Valid settings for the audio level are from 0 to 4, where 0 means "mute".
Service Center Number: full phone number.
In order for the SMS facility to operate, you must set the correct number. This is the SMS center of the GSM operator. Enter the phone number of the GSM carrier between quotes, like "+40722004000".

The "SMS" options that follow let you send or receive SMS messages from your computer to any GSM mobile phone user, through the HSDPA module of the BYTTON equipment cell phones.

5.7.3. SMS Read

Displays a list of received text messages.



This list for displaying received SMS messages has the following columns:

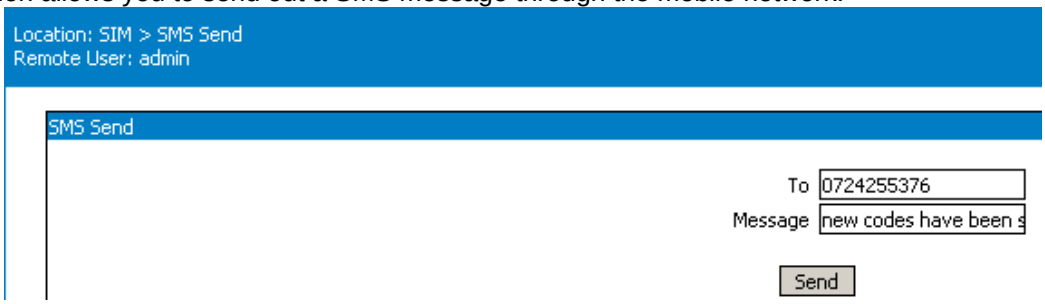
- ID : reference number: 1, 2, and so on up to 14;
- STATUS: REC(Received), READ or UNREAD;
- FROM: sender's phone number, such as "+40728592243";
- DATE: date and time when the message was recieved(after the "+" sign the tenths of seconds);
- TEXT: the actual content of the message.

You may delete one or several messages by typing the index number in the box at the bottom and clicking "Go".

Note: When the maximum storage capacity of 15 messages is reached the BYTTON won't be able to receive newer SMS.
If you want to continue receiving messages, you must delete some of the older SMS.
After deletion, click "SMS Read" to collect your new messages from the server.
The new message will be displayed, at first at the bottom of the list, and upon next "Read" command it will be sorted upon the "ID" field and placed in its proper(cronological) position.

5.7.4 SMS Send

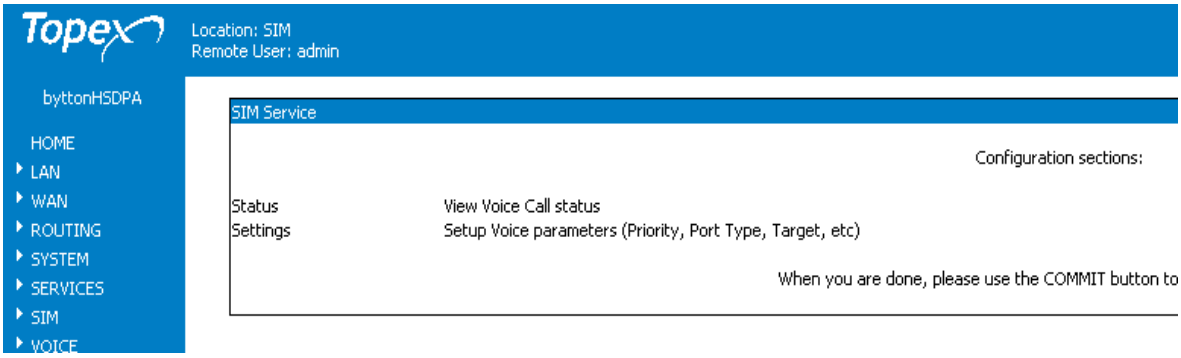
This option allows you to send out a SMS message through the mobile network.



Just type in the destination phone number in the field "To" and the text you want to transmit in the "Message" field , then click the Send button.
Wait about 40 seconds for the mobile network to perform the sending operation.
If the SMS cannot be send (network busy, congestion or other problems), an error messages will appear on top of the screen.
Note: if the phone number for the SMS destination is in the same network, you may enter it in short form, as above. But if it is in a different mobile network, you must type it in full format: country code, area code, number, for example "+40747999999".

5.8. VOICE

Configure the phone interface and routing of calls.



There are two configuration pages in the voice section:
Settings, which allows you to select the priority of voice calls, type of the phone interface and the routing of incoming calls (target, DISA, extension);
Status , which shows the current state of the voice interface of your Bytton device (on hook, in call, stopped, and so on).
To understand these settings, you must first review the modes of connecting BYTTON to a PBX or a phone.

5.8.1. Phone Connections for BYTTON HSDPA

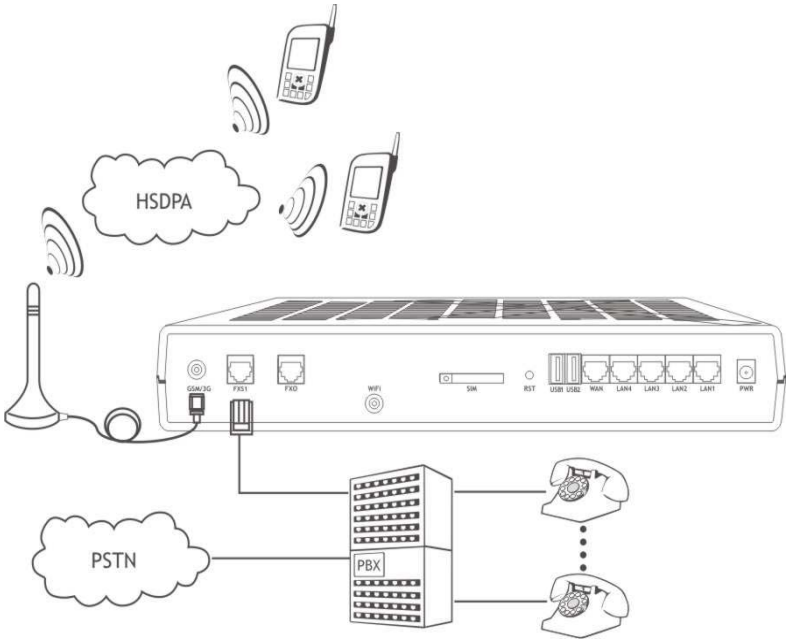
The telephony interfaces of BYTTON HSDPA can be connected in several ways:

- to an analogue trunk of a PBX exchange
- directly to an analogue phone
- to a local interface (office subscriber) of PBX exchange

For this purpose BYTTON HSDPA has two interfaces with RJ11 connectors, one is for FxO connection and the other for FxS connection.
Only **one of them** may be connected at any moment of time!
The selection is done through the Web interface, in the "PHONE" subsection, where you must set the phone line interface **either** as FXS or as FXO.

Connecting to a PBX trunk or a telephone

Use the FXS interface of BYTTON HSDPA (which must be activated from the Web configuration page VOICE Settings), as shown in the drawing below:



Incoming call

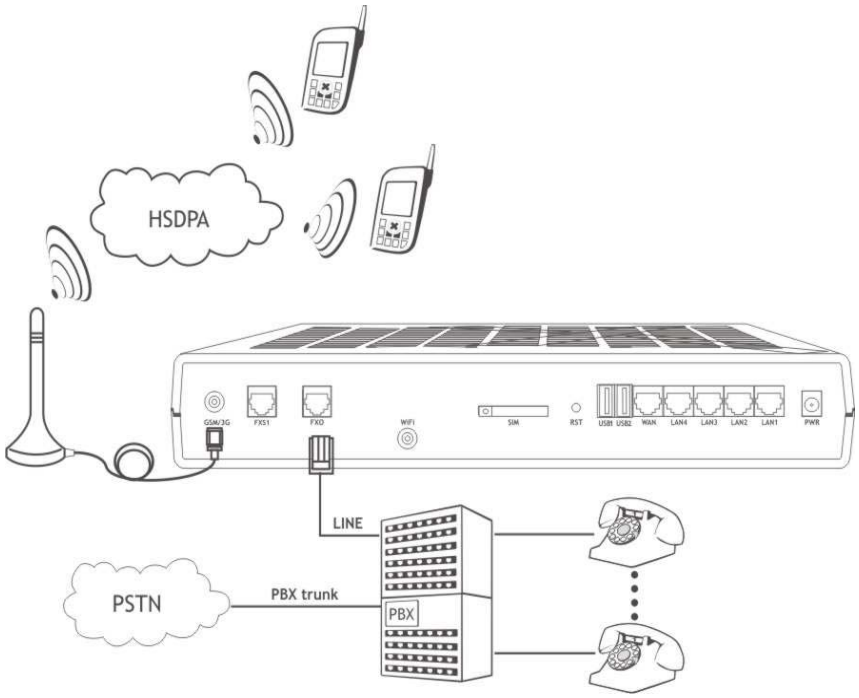
BYTTON HSDPA interface receives a call over GSM/GPRS/EDGE/HSDPA network. The equipment sends a call signal to the analogical phone that is connected or to the PBX exchange; in the second variant the exchange switches the call a local subscriber.

Outgoing call

PBX exchange must be configured to output the calls through BYTTON HSDPA. The user simply dials the wanted number from an office telephone.
PBX exchange processes the number and analyses the prefix and sends it to the outgoing trunk where BYTTON HSDPA is installed. Then BYTTON HSDPA transmits the call to the mobile network.

Connecting to an extension of PBX

For this the FxO interface of BYTTON HSDPA is used, also properly enabled.



This kind of connection is very useful especially when there are no available analogue trunks: for instance PBX exchange is entirely configured as ISDN type or it has no more free analogue trunk (all of them are busy).

Incoming call

- **with DISA (Direct Inward Service Access)**

A call is received from the mobile network.

BYTTON HSDPA answers and opens a local line. The PBX exchange generates a dial tone. On this tone, the caller dials the number: a local extension or an external number. The PBX exchange routes this call in the same way as it treats any call came from a **local** subscriber.

- **with automatically routing to a Target**

A call is received from the mobile network.

BYTTON HSDPA answers and opens a local line. The PBX generates a dial tone. On receiving this tone, BYTTON assigns it a specified local extension (programmable Target Number). The engaged extension rings and the call over mobile network is established. The local extension can be, for instance, the operator panel who answers and directs manually the incoming calls.

Outgoing call

The user dials the number of local interfaces, where BYTTON HSDPA is connected.

BYTTON HSDPA answers and generates dial tone. After the recovering this tone, the caller dials the number of mobile network subscriber. BYTTON HSDPA transmits the reading and makes the link with mobile network.

Test calls

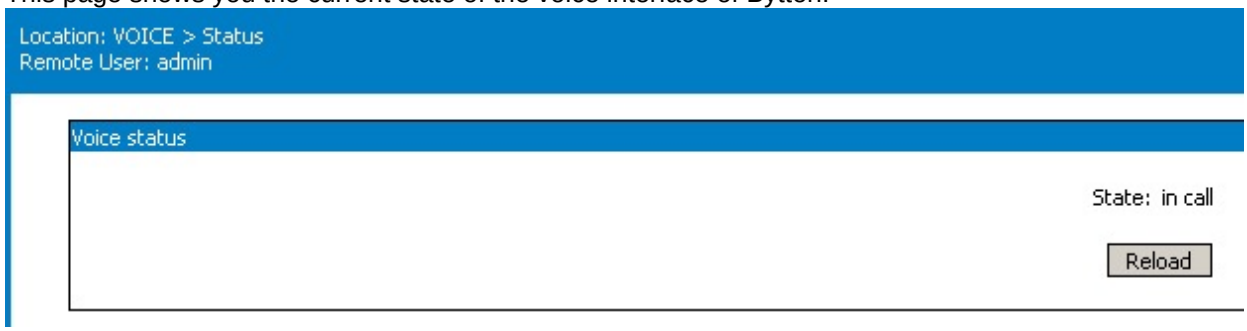
For all the configurations shown above, it is recommended that you make first some test calls, to verify that the BYTTON HSDPA equipment operates correctly.

Note: If you want to be able to use the voice phone connection, after you have performed the required settings and pressed "Commit", check that the GSM/GPRS/EDGE/HSDPA module is properly registered to the 3G network. Verify that the 3G led blinks twice in quick succession to show correct registration. Otherwise you will have no voice connection and hence no dial tone when you pick up the phone connected to BYTTON HSDPA. It is possible that you have a good data connection, and can you surf the Net or download files over the HSDPA broadband network, but the voice service is not available for the moment!

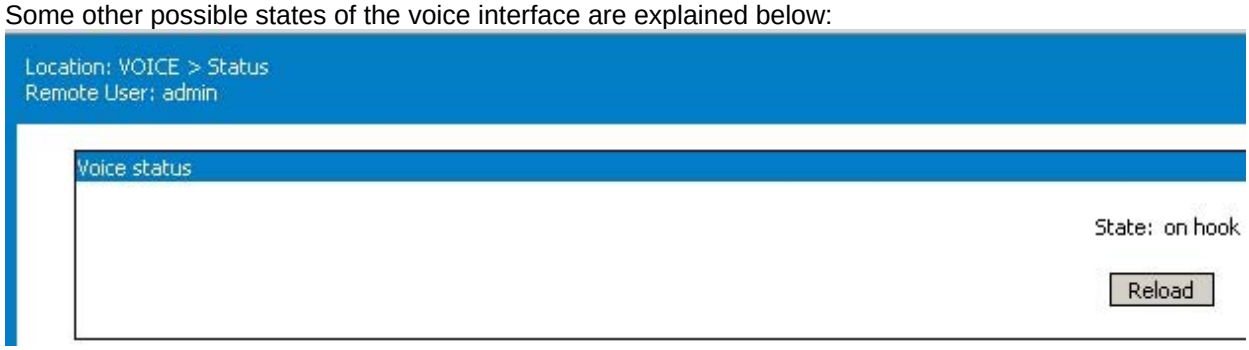
Also, when you perform the Voice Interface settings for, take into account the warnings and recommendations shown in the respective paragraph.

5.8.2. VOICE Status

This page shows you the current state of the voice interface of Bytton.

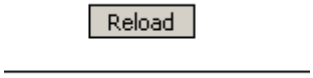


The example above indicates that the voice port of the BYTTON equipment is in a call.
Some other possible states of the voice interface are explained below:

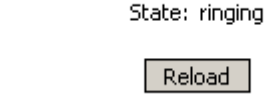


When you don't use the voice connection, this should be the normal state: the handset in put down (on hook), the phone interface is not active.

You have picked up the handset, prior to dialing a number, or the phone exchange has engaged the junction where Bytton is connected. The phone line becomes active.



There is a call coming in, the phone port is in its RING phase. You should pick up the handset to answer the call.

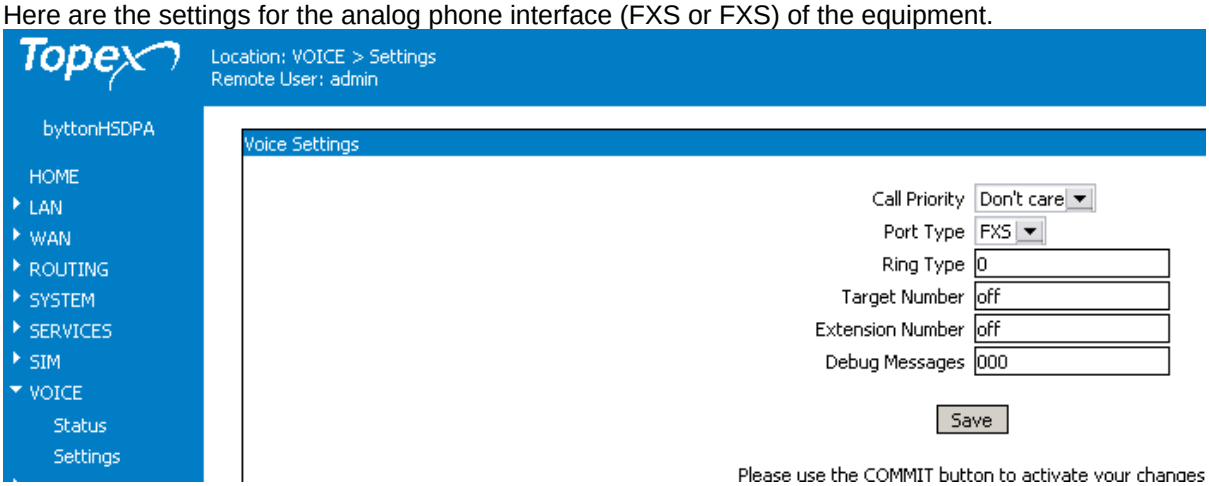


The voice state shows "stopped" when the voice connection is temporary unavailable (lack of signal, no registration, other reasons). In this case, you will hear in your headset a busy tone, indicating that you cannot make voice calls!

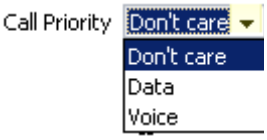
The "stopped" problem may be temporary. For example, the SIM may not be properly registered, the RF signal is weak or the network is busy.
Try to call again later or reset the Bytton equipment to re-activate the voice connection.

5.8.3. VOICE Settings

Here are the settings for the analog phone interface (FXS or FXS) of the equipment.



Call Priority:
Establishes which kind of call has higher priority, Data or Voice.
The default is "Don't care". This setting is important for 2G networks (such as GSM, GPRS, EDGE) where you can't have voice and data connection **at the same time**. Then you must set a priority.



If you set the call priority to **Voice**, then when you try to make a voce call, Bytton will stop the ongoing data connection to allow you make the call.
If you set the priority to **Data**, the data traffic will interrupt an voice call already established.

Note: *In case of 3G networks (UMTS, HSDPA) that support **simultaneous** voice and data calls there is no need to impose a priority, so you should leave the setting on the default value "Don't care"*
Port type: first of all, you must choose the type of the phone port to use. You can select either FXS (for connection to a trunk of the PBX or directly to an analog phone) or FXO (when BYTTON HSDPA may be connected to a local extension of the PBX, as you would connect a standard office phone). The default is FXS.
Ring type: select the type of ring signal. The default value "0" means a standard ring current, frequency 25 Hz, symmetrical (with no DC component). The value "1" selects a ring current with DC component, thus asymmetrical. This vas requested for certain types of phones, which won't ring properly with a symmetrical ring current.
Target Number - specifies how the incoming calls should be treated, in case of phone interface configured as FXO.
The default is off, or you should type a phone number (up to 4 digits).
When a call comes in through the FXO interface, you have two options: either provide the caller with DISA tone, allowing him to dial numbers in DTMF mode, or specify a Target number. In the latter case the DISA feature is not used, instead the incoming call is routed directly to the local extension established in the Target Number field. For instance, this extension may be the attendant console, so the operator will route the calls manually.

Extension number – the number of the local extension where the Bytton equipment is connected, in case of configuration as FXO,.

Debug messages: establishes the type of debug messages that will be sent to the Log file.
Valid values are from 000 (the default, no messages are sent) to 111 (full debug, all messages will be sent). These messages are useful for troubleshooting. There is no need of them for making voice calls.

In the paragraph 5.5.2, about the "System Log", you can see the influence of selecting a value of 111 for the debug messages, as opposed to the default 000.

Warning, unauthorized voice access is possible! *In case of telephone interface configured as FXO, unauthorized voice access is possible. If there are no restrictions regarding the access rights of the extension where BYTTON HSDPA is connected, anyone who calls the mobile number of the BYTTON HSDPA from a public network will get access to the outgoing lines of the PBX. He will be able to make long distance calls that will be charged to the owner of the phone exchange.*

To avoid this risk you have two possibilities:

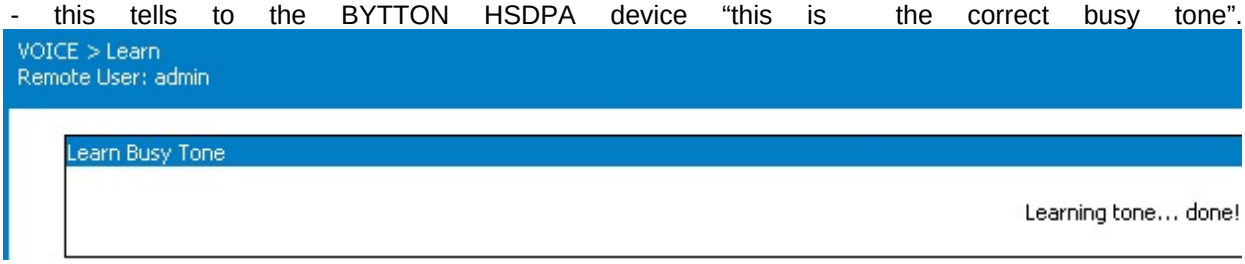
1. Either configure the PBX to reject the outgoing calls that are initiated from the extension where the BYTTON HSDPA interface is connected.
2. Or, if the exchange cannot be configured in that way, then you must set the BYTTON HSDPA equipment **not** to offer a DISA tone when a mobile phone call coming in. Instead, specify a "Target Number" instead of providing DISA tone. The PBX will route the call to the operator. Instead of leaving the "Target Number" on the default "off" value, enter the number of the operator desk.

Learn Busy Tone:

This setting refer to the requirement that the Bytton phone port, used as FXO interface, remembers correctly the "busy" tone of the PBX. Different private phone exchanges may have different "busy" tones, so you must teach the Bytton HSDPA equipment how to identify a local busy tone.

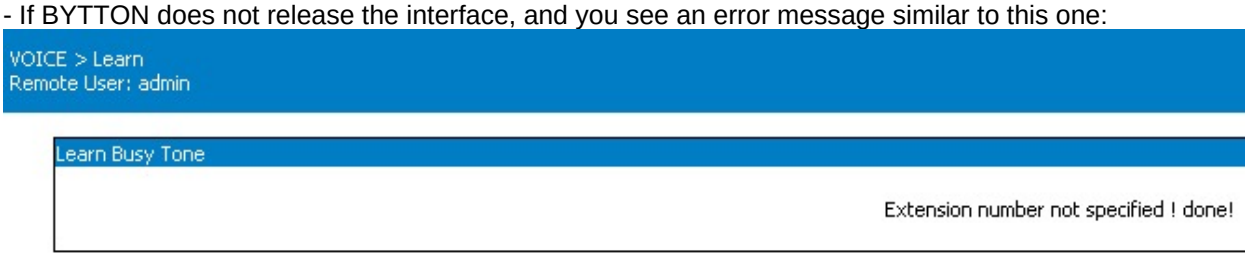
In order to monitor the busy tone, the interface must be „told" how to identify the busy tone of the particular phone exchange where it is connected. Here is how you must proceed:

- set the line type as FXO and connect BYTTON to a local extension;
- perform a "Save";
- make a call to the respective extension, from another local phone of the PBX where the BYTTON equipment is connected;
- Bytton will answer the call;
- than hang up the extension from where you made the call. This way a busy tone will be generated towards the extension where the BYTTON device is connected;
- the interface (junction) is released, following a time interval, by the BYTTON equipment. Check if FXO interface is released after a few seconds and click "Learn Busy Tone";
- this tells to the BYTTON HSDPA device "this is the correct busy tone".



If you see the message "Done!", it is OK, so perform "Save" again.

- If BYTTON does not release the interface, and you see an error message similar to this one:



you should start over again the learning process.

Warning! *It is **strongly recommended** that you use "Learn Busy Tone".*
Without it, the BYTTON equipment cannot sense when the subscriber that called has hang up, and the PBX has send "busy" tone. If the called party is a human being using a cell phone, he will hear the busy tone and should hang up. But if the correspondent is another equipment such as Bytton, it won't realize that the call has been ended, and the link will remain on. Consequently, the phone bill will be huge!
To prevent this from happening, you should use the "Busy Tone Detection" option.

5.9 Optimizing WiFi Performances

This paragraph shows you a few basic suggestions for improving the performance of the wireless network of the BYTTON HSDPA router.

5.9.1. Network physical configuration

As a general rule, you should try to locate the BYTTON HSDPA equipment and their wireless clients away from sources of EMI disturbances. These sources can be heavy-duty electric motors, heaters, transformers, fluorescent lights, microwave ovens, refrigerators, radio and TV equipment, etc.
To improve coverage, install the BYTTON HSDPA Routers in open areas. If this can't be done or the distance between the wireless base station and its clients is too large, you should use additional WiFi Access Points as needed, to obtain adequate signal strength through your building. Even BYTTON itself may be used as transparent bridge (repeater) located midway between an AP and a remote client.
There are appliances (microwave ovens) that operate in the same frequency band as the AP of BYTON Router. Thus your network performance may decrease when you use a microwave in the range of the WiFi of BYTTON HSDPA. This does not mean operation is impossible, both your microwave and your the Bytton wireless Router will continue to function.

5.9.2. Range

Before installing/setting up a BYTTON HSDPA router, it is recommended to perform a **site survey**. Without this it is not possible to determine the exact range that will be achieved and the number of auxiliary APs required for a good coverage. Each office or home environment is unique because of different topologies, size and shape of rooms, materials, and so on.

Please remember that:
- the specified transfer rate is the speed at which individual bits of data flow through a channel, not necessarily the speed at which entire files are uploaded or downloaded
- these actual speed may vary, and often will be less than the maximum data rate
- wired or wireless speeds are affected by several factors including the availability of Internet routers, the level of loading of the 3G cell, the capacity of and services offered by your mobile network service provider, channel capacity, network traffic, computer equipment, type of server, number of connections to server, etc.

In the frequency bands used by WiFi, radio signals may be absorbed (damped) by some obstacles or reflect off of other obstacles, depending on their construction. The standard specifications for 802.11b devices guarantee "up to 350 m in open space". This is achieved outdoors where the two devices see each other with no obstacles (they have a line of sight).

Still, the same two units may only achieve up to 100 m of range when used indoors. Heavy concrete or metal walls may decrease this range even further.

Also, the IEEE 802.11b specification supports four data rates: 11 Mbps, 5.5 Mbps, 2 Mbps, and 1 Mbps. Operation at 1 Mbps provides greater range than operation at 11 Mbps and so on. The BYTTON HSDPA Router will automatically adjust the data rate to maintain a usable radio connection.

This means that a WiFi client that is close to the Bytton wireless Router may operate at rates of 11 Mbps while a client that is on the far limit of coverage area will only operate at 1 Mbps.

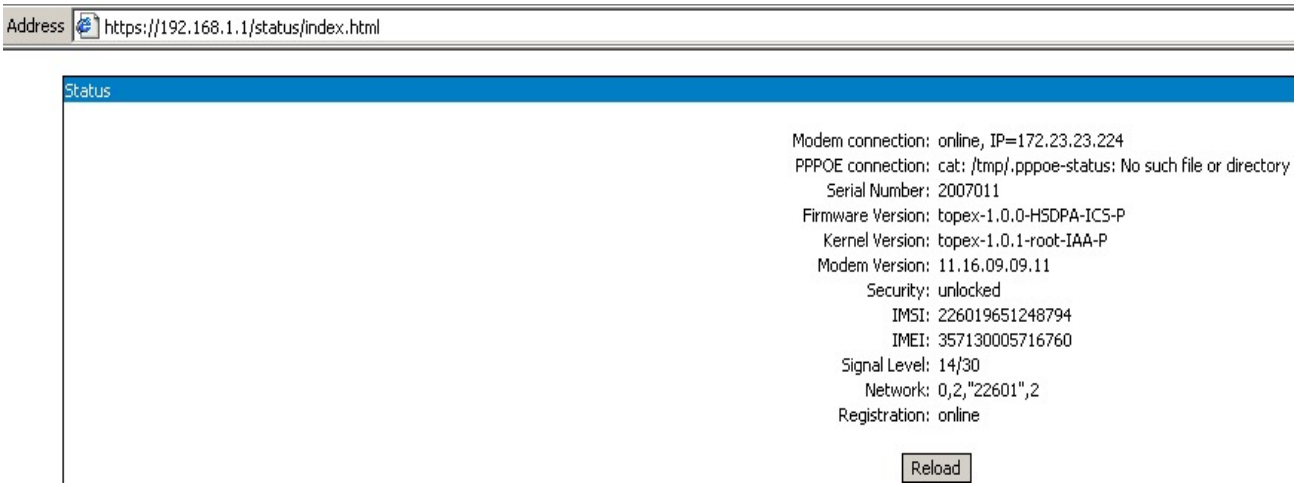
If you want a very high data rate, the effective wireless range of the BYTTON Router will be reduced.

The same considerations hold true for the specification IEEE 802.11g: the maximum data rate (54 Mbps) can be reached only if the signal strength is good enough. This means the typical range in an office building may be just 20 m if you insist upon a 54 Mbps throughput, but it will increase to 50 m if a transfer rate of 11 Mbps is acceptable for you.

Precisely because of their higher data rates, 802.11 g devices may be more susceptible to interferences!

5.10 Status Page

The Bytton HDSPA router features a **status page**, accessible for any user without need for administrative password. Just enter in your browser the URL for the page: ""https://192.168.1.1/status" or https://192.168.1.1/status/index.html



While the configuration web pages shown previously are for **configuring** the BYTTON HSDPA equipment, and are accessible only with log-in (you have access if you enter the correct user name and password), the Status Page can be accesses by any user.
It shows you the essential parameters of the Topex wireless router, that are available in the web pager "SIM Status" and "System Status" described previously.

Data connection: it may be offline, online or stopped. If it is online, it also shows the current IP on the WAN side, such as "172.20.36.180" or "172.23.4.4299".
You may have, as in this example, a SIM registered online, the mobile network is available for voice calls, but the modem connection is offline, you cannot connect to Internet via HSDPA modem.
You can see also info about the Ethernet link or PPP link.

PPPoE connection: information about the data link using PPP over Ethernet. In the above example, the status for the PPPoE connection is not yet available, so you see this error message.
Serial number: Each Bytton device from Topex has an unique serial number, such as 0707211, 15, 17 and so on.
Firmware version: version of the firmware running on BYTTON: you may see "Firmware version is 0.6.3" or "topex-1.2.3–NETWORK-xyz-P" in the above example, and so on.
The three digits following the name "topex" show the version of the application program running, such as 0.7.2 or 1.0.0, NETWORK identifies the mobile network used (GPRS, EDGE, CDMA, HSDPA, EVDO, TDD and so forth), while the three letters detail the platform, the modem type and the version (standard, dedicated for a certain carrier, with hard disk drive, etc). Finally, the last letter indicates the type of the case, P for plastic or M for metal;
Kernel version: The new equipments use distinct Flash memory partitions for the operating system (kernel) and for the application programs, making the product more versatile and more robust. The two memories may be updated separately, according to the requirements of the users. The memory for the operating system is write-protected, thus in case of problems, accidental erasure or power failure during updating, you still have a "kernel" that allows you to load a new software image;
Modem Version: code describing the version of the embedded firmware of the mobile modem of the BYTTON equipment; it is useful for debugging.

Security: the state of the SIM card. Normally it should be "unlocked", if it is "Locked by PIN" it means you must enter the correct PIN code in order to unlock it.
- **IMSI** (International Mobile Subscriber Identity), identity of the subscriber
- **IMEI** (International Mobile Equipment Identifier). 15-digit number that uniquely identifies an individual mobile terminal wireless device such as the HSDPA modem of BYTTON

– **Signal Level**, displayed with four figures separated by a bar. The two digits indicate the level of the RF signal for the GSM/GPRS/EDGE/UMTS/HSDPA network on a scale from zero to 30. The higher the
– **Network**: the name of the mobile network where the equipment is registered, as transmitted by the mobile carrier value, the better 3G signal you have.
- Registration status: shows if the SIM card of the equipment is registered to the mobile network (online) or not. Of course, if the SIM is not present, not activated or the signal level is much too low, the network-related information cannot be displayed.
– But the information related to the equipment (firmware version, version of the HDSPA modem, IMEI code) will still be shown on the screen.
– If the SIM is active and the signal is above zero, it will show IMSI and network information, even if not properly registered with the mobile carrier (you cannot make voice or data calls).

5.12 KERNEL MODE

The Topex Bytton HSDPA uses an advanced architecture, using two distinct Flash memory chips .

While the usual architecture, with a single flash storage chip for the equipment, when an error occurs during the update process, the operation of the device can be compromised. It does not boot up, no more simple upgrade via web page is possible, so it required needed expert assistance in order to re-load the firmware.

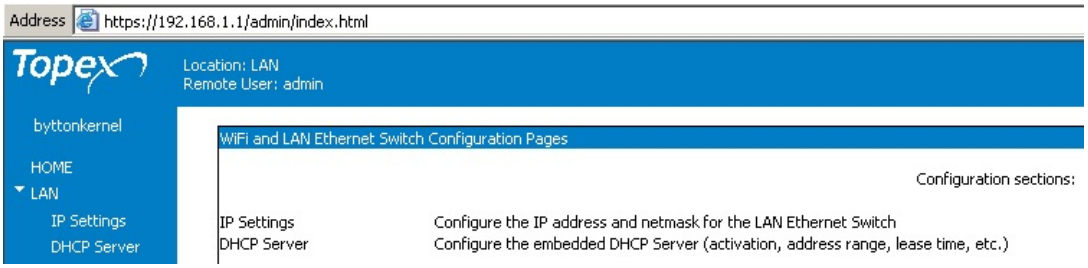
For this reason, now Bytton uses two **separated** partitions on the storage media (Flash memory). One is for the application, the user-specific software that is easily upgraded, while the other is reserved for the operating system of the equipment (the "kernel"). This partition is write-protected, so in cannot be damaged. Thus, even if there is a power failure or other problem during updating, only the application part is lost, the operating system of Bytton remains still available, allowing you to update the software.

The "System Status" window shows this structure, displaying on two consecutive rows the firmware version (applications programs) and the kernel version (operating system of BYTTON).

Owing to this dual-flash architecture, when the application part of the firmware is deleted, or becomes corrupted, you will still be able to connect to Bytton HSDPA.
You will see on the screen the shortened variant - notice the name "byttonkernel" instead of the usual "byttonHSDPA" below the Topex logo.

This "kernel" web page has only the settings "LAN" and respectively "System".
The kernel functions allows you to:
- change the IP address (this includes, besides the address itself, the DHCP)
- save and load a configuration
- update the application part of the firmware.

5.12.1 LAN



The settings for the LAN side of the network, that is IP configuration and respectively DHCP configuration.
No settings for WiFi are available here!

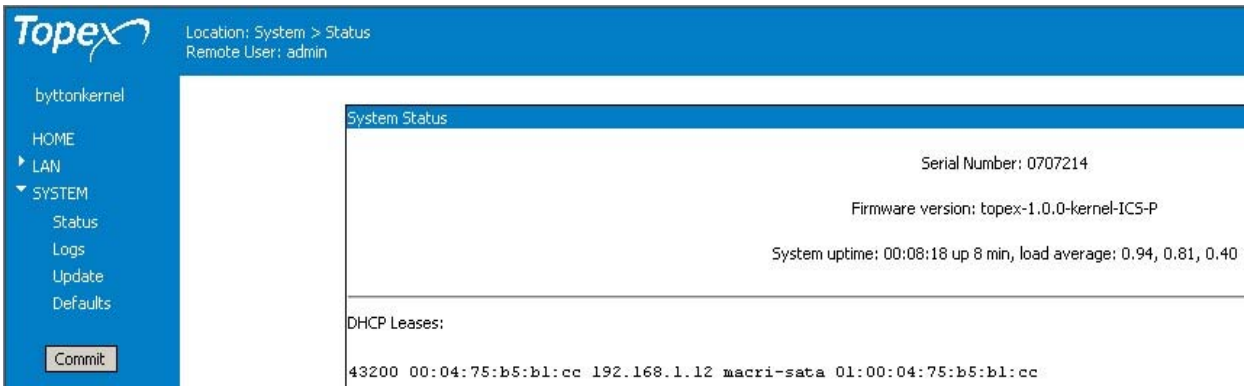
IP

Same as the normal LAN settings, described previously. The default value of the local IP address is 192.168.1.1 and the netmask is the standard one, 255.255.255.0. The network mask allows limiting the accessibility domain for the address above.

DHCP

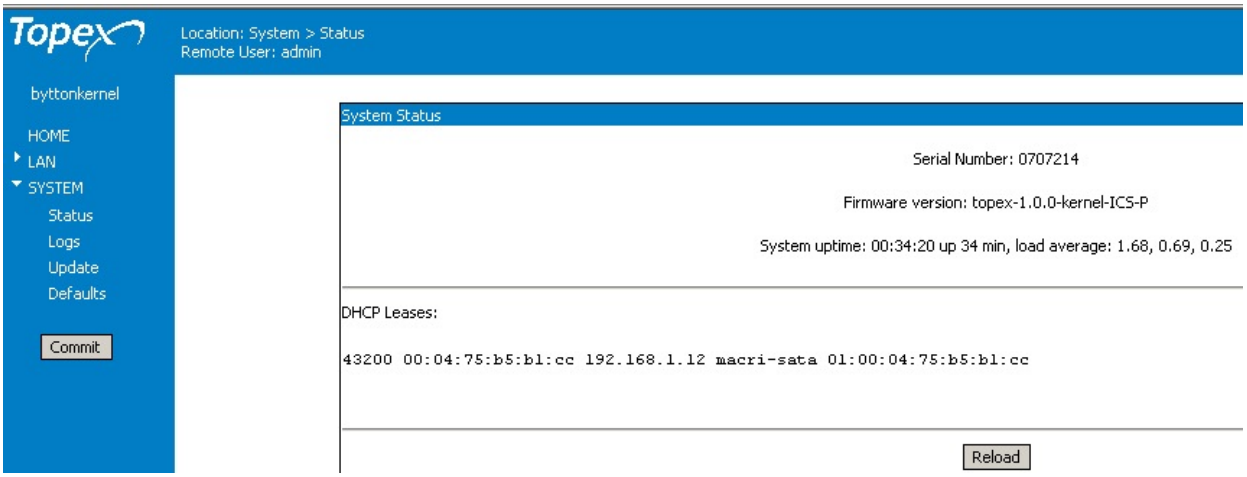
The settings are Identical with the DHCP settings in the normal configuration of Bytton HSDPA.
If you enable the Dynamic Host Configuration Protocol feature, our Bytton equipment may can be used as a DHCP server for your local network.
You should leave the DHCP feature to Enabled and DNS Servers to Automatic.
For configuration details, please se paragraph 5.2.4.

5.12.3 System



The System section has only these pages: Status, Logs, Update and respectively Defaults.

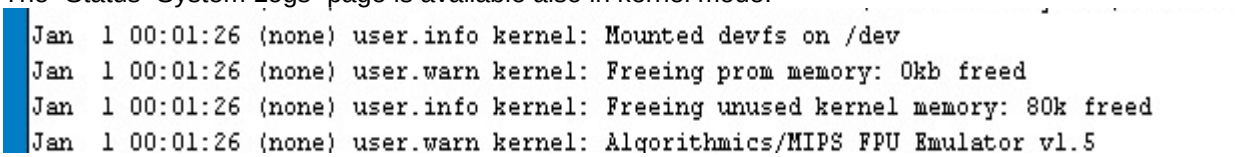
Status



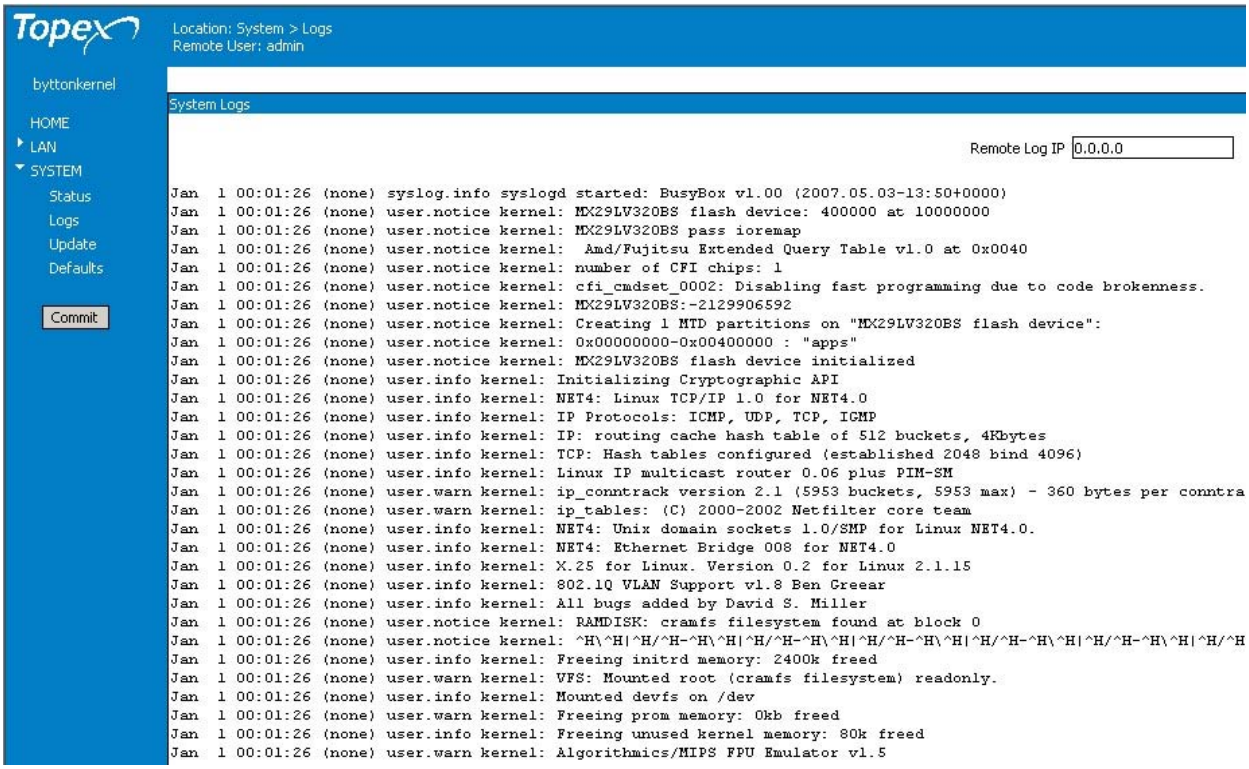
In Kernel mode, the Status windows shows the following information:
- serial number of the equipment
- firmware version (the version of the kernel for the device)
- system uptime and load averages
- DHCP leases.

Logs

The "Status>System Logs" page is available also in kernel mode:


Jan 1 00:01:26 (none) user.info kernel: Mounted devfs on /dev
Jan 1 00:01:26 (none) user.warn kernel: Freeing prom memory: 0kb freed
Jan 1 00:01:26 (none) user.info kernel: Freeing unused kernel memory: 80k freed
Jan 1 00:01:26 (none) user.warn kernel: Algorithmics/MIPS FPU Emulator v1.5

While Bytton HSDPA works in Kernel mode, only kernel-related messages (user info, notices and warnings) will be displayed, since the application software is not present.
Also, since no Internet connection is available for updating the time, the date/time of the logs will always be Jan 1:


Topex
Location: System > Logs
Remote User: admin
byttonkernel
HOME
LAN
SYSTEM
Status
Logs
Update
Defaults
Commit
System Logs
Remote Log IP 0.0.0.0
Jan 1 00:01:26 (none) syslog.info syslogd started: BusyBox v1.00 (2007.05.03-13:50+0000)
Jan 1 00:01:26 (none) user.notice kernel: MX29LV320BS flash device: 400000 at 10000000
Jan 1 00:01:26 (none) user.notice kernel: MX29LV320BS pass ioremap
Jan 1 00:01:26 (none) user.notice kernel: Amd/Fujitsu Extended Query Table v1.0 at 0x0040
Jan 1 00:01:26 (none) user.notice kernel: number of CFI chips: 1
Jan 1 00:01:26 (none) user.notice kernel: cfi_cmdset_0002: Disabling fast programming due to code brokenness.
Jan 1 00:01:26 (none) user.notice kernel: MX29LV320BS:-2129906592
Jan 1 00:01:26 (none) user.notice kernel: Creating 1 MTD partitions on "MX29LV320BS flash device":
Jan 1 00:01:26 (none) user.notice kernel: 0x00000000-0x00400000 : "apps"
Jan 1 00:01:26 (none) user.notice kernel: MX29LV320BS flash device initialized
Jan 1 00:01:26 (none) user.info kernel: Initializing Cryptographic API
Jan 1 00:01:26 (none) user.info kernel: NET4: Linux TCP/IP 1.0 for NET4.0
Jan 1 00:01:26 (none) user.info kernel: IP Protocols: ICMP, UDP, TCP, IGMP
Jan 1 00:01:26 (none) user.info kernel: IP: routing cache hash table of 512 buckets, 4Kbytes
Jan 1 00:01:26 (none) user.info kernel: TCP: Hash tables configured (established 2048 bind 4096)
Jan 1 00:01:26 (none) user.info kernel: Linux IP multicast router 0.06 plus PIM-SM
Jan 1 00:01:26 (none) user.warn kernel: ip_conntrack version 2.1 (5953 buckets, 5953 max) - 360 bytes per conntra
Jan 1 00:01:26 (none) user.warn kernel: ip_tables: (C) 2000-2002 Netfilter core team
Jan 1 00:01:26 (none) user.info kernel: NET4: Unix domain sockets 1.0/SMP for Linux NET4.0.
Jan 1 00:01:26 (none) user.info kernel: NET4: Ethernet Bridge 008 for NET4.0
Jan 1 00:01:26 (none) user.info kernel: X.25 for Linux. Version 0.2 for Linux 2.1.15
Jan 1 00:01:26 (none) user.info kernel: 802.1Q VLAN Support v1.8 Ben Greear
Jan 1 00:01:26 (none) user.info kernel: All bugs added by David S. Miller
Jan 1 00:01:26 (none) user.notice kernel: RAMDISK: cramfs filesystem found at block 0
Jan 1 00:01:26 (none) user.notice kernel: ^H\^H|^H/^H-^H\^H|^H/^H-^H\^H|^H/^H-^H\^H|^H/^H-^H\^H|^H/^H-^H\^H|^H/^H
Jan 1 00:01:26 (none) user.info kernel: Freeing initrd memory: 2400k freed
Jan 1 00:01:26 (none) user.warn kernel: VFS: Mounted root (cramfs filesystem) readonly.
Jan 1 00:01:26 (none) user.info kernel: Mounted devfs on /dev
Jan 1 00:01:26 (none) user.warn kernel: Freeing prom memory: 0kb freed
Jan 1 00:01:26 (none) user.info kernel: Freeing unused kernel memory: 80k freed
Jan 1 00:01:26 (none) user.warn kernel: Algorithmics/MIPS FPU Emulator v1.5

As mentioned previously, the log is very useful for debugging.

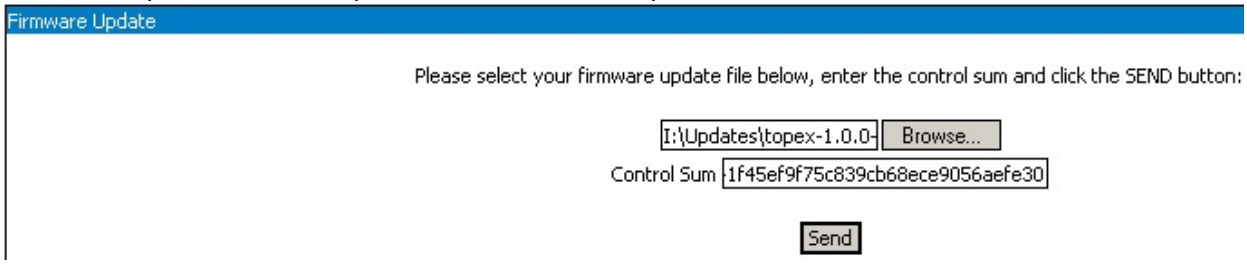
Update

The most important function of the Kernel mode is firmware update: you can load a new version of the application program, to get the equipment fully operational.
Click "Update" then select the image file to upload.

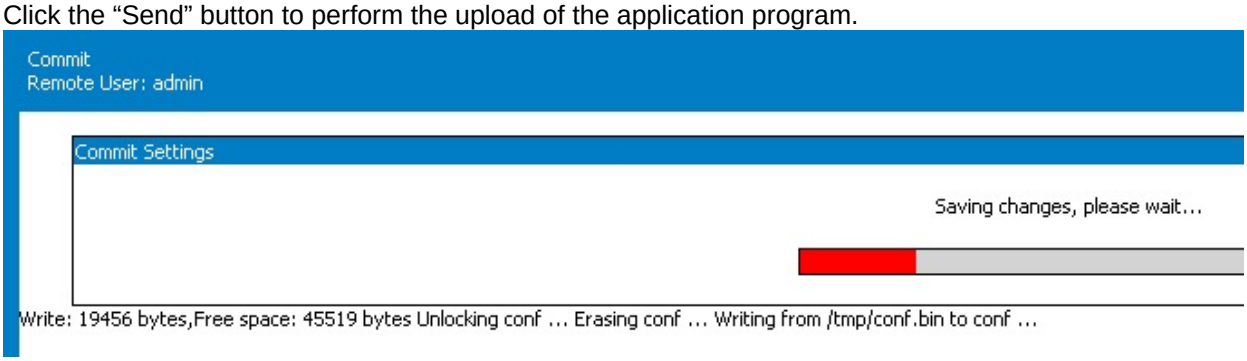
*Remember that each firmware file has a **Control Sum** associated with it, and it won't be loaded if the control sum does not check out. This feature ensures that you will not load a image file that become corrupted, because such a corrupted firmware could prevent operation of your BYTTON equipment. The control sum is a string of hexadecimal figures, such as "41f45ef9f75c893468511a64f21273e713fe30" which is stored in a text file (with .txt extension), with the same name as the firmware image.*

BYTTON asks you for the name of the firmware file and the associated control sum. For this, first go to the text file with the same name as the firmware image you want to load and open this file with Notepad (or other file editor utility).
Copy the control sum (with Ctrl-V or Edit>Copy) and then go to the firmware image file (with the extension .trx) to select it.

Enter the copied control sum (with Ctrl-C or Edit>Paste) in the field "Control Sum":



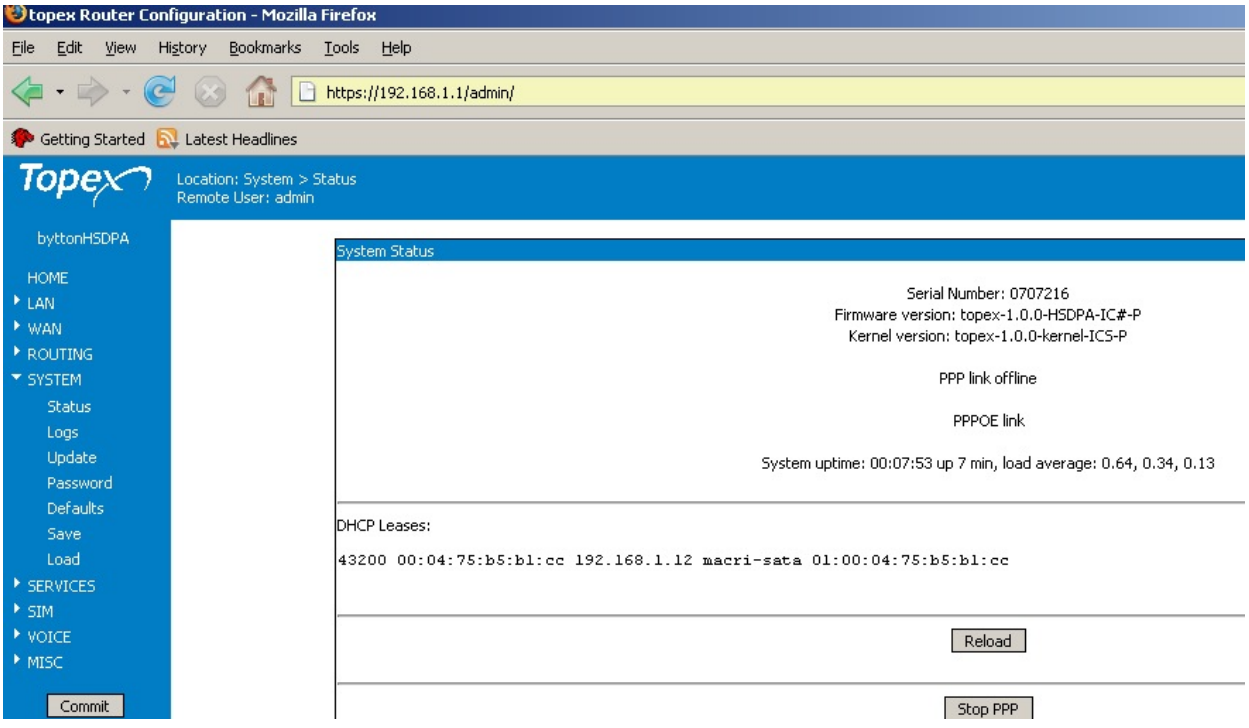
Click the "Send" button to perform the upload of the application program.


Commit
Remote User: admin
Commit Settings
Saving changes, please wait...
Write: 19456 bytes,Free space: 45519 bytes Unlocking conf ... Erasing conf ... Writing from /tmp/conf.bin to conf ...

The equipment checks the image file versus its control sum, and if it is OK, it writes the application program into the Flash memory. Besides the red indicator progress, you will see messages such as "unlocking", "erasing", "writing" which show the different phases of the process of upload for the application software.

While loading a new program image (also when committing changes or when resetting to defaults), the Bytton equipment will cease operation for a few seconds. This means all connections: data link, voice, LAN and WiFi will be interrupted, then will resume when BYTTON starts again.

After the restarting of the equipment, you should go to System Status to confirm that the application firmware has successfully loaded and is in operation:



Now you should see:
- under the TOPEX logo, the name "byttonHSDPA";
- in the column to the left, all the items of the Menu are present (Besides LAN and System available in kernel mode, now there are also WAN, ROUTING, SERVICES, SIM, VOICE, MISC and so on);
- information about both firmware version and kernel version;
- information about the active Internet connection (Ethernet, PPP link or PPPOE)
- Reload and Stop PPP/Start PPP buttons.

6. TECHNICAL SPECIFICATIONS

Title	Description
Mobile networks supported	GSM/GPRS/EDGE and respectively HSDPA/UMTS
Frequency bands	GSM/GPRS/EDGE: 850/900/1800/1900 MHz HSDPA/UMTS 2100MHz: 2100 MHz (Band Class 1)
Supported protocols	TCP/IP, PPP, CHAP, PAP, ARP, UDP, RIP v.2, NTP and others
Features	Full Firewall (SPI) Router Auto-negotiation, Auto-crossover Switch 4+1 switch DHCP Server Web configuration GRE for IP tunneling Quagga with RIP or OSPF for dynamic routing
Wired Network interfaces	Four LAN ports Ethernet 10/100 base-T One WAN port Connector type: female RJ45 Supports both static and dynamic IP address Transfer speed: 10/100 Mbps
Wireless Access Point	Supports the 802.11b/g WiFi standard Maximum bandwidth: 54 Mbps for g, 11 Mbps for b Frequency range: 2.4 GHz Fully configurable via Web page
Voice interfaces	Phone interfaces, either FXS or FXO Line voltage :48Vcc 10%, Line current: 30 mA max. Ring signal: 25 Hz, min. 65 V rms, programmable DC component; Impedance: 600 ohm Connector type: female RJ11
High speed wireless modem	Simultaneous Voice and data (for networks that support this feature) Stable and reliable concurrent service: supporting concurrency of voice service based on UMTS and data service based on packet switched (PS) mode; Supporting SMS service based on GSM, GPRS, EDGE or UMTS, supporting group transmission of messages GPRS: Multi-slot Class 10, type B, maximum: 4 slots RX, 2 slots TX, 5 slots Active, up to 85.6kbps on the GPRS network EDGE: Multislot class 10, Link Adaptation and Incremental Redundancy, up to 236 Kbps Download and 118 Kbps Upload UMTS data: PS, speed 384 Kbps Download and Upload HSDPA data: 3GPP R5 2004/06, up to 1.8Mbps Download and 384 Kbps Upload
Packet access	One-phase and two-phase access for GPRS and EDGE
Max. transmitter power	GSM/GPRS/EDGE 850/900MHz: +32dBm (Power Class 4) GSM/GPRS/EDGE 1800MHz/1900MHz: +29 dBm (Power Class 1) UMTS/HSDPA 2100MHz: +23dBm (Power Class 3. 8PSK mode Class E2)
Receiver static sensitivity	GSM/GPRS/EDGE 850/900: - 107 dBm 1800/1900MHz: -105 dBm Compliant with TS 05.05 (R99) UMTS/HSDPA 2100MHz: Compliant with 3GPP TS 25.101(R5)
Voice service	GSM: FR, EFR, HR, AMR UMTS: AMR(12.2kbps/10.2kbps/7.95kbps/7.4kbps/6.7kbps/5.9kbps /5.15kbps/4.75kbps)

Detailed data services	GSM CS: UL 9.6kbps/DL 9.6kbps GPRS: UL 42.8kbps/DL 85.6kbps UMTS CS: UL 64kbps/DL 64kbps UMTS PS: UL 384kbps/DL 384kbps UL UMTS/DL HSDPA: UL 384kbps/DL 1.8Mbps *Note: these are the uppermost limits of the 3G+ technology under laboratory conditions, you may not reach these speeds on your premises.*
Concurrent service (Based on UMTS)	1 UMTS CS voice + 1 UMTS PS data
SMS	Supporting SMS based on CS domain of GSM or UMTS Supporting SMS based on PS domain of UMTS
HSDPA antenna	External quad-band antenna with magnetic base and cable
WiFi antenna	External stick antenna for 2,4 GHz
Supply voltage	12 $V_{D.C.}$ (+ center wire, - external conductor) Dee Van Enterprises Ltd. Type: DVE DSA-30PF-12
Supply adapter	Special adapter, output : 12 $V_{D.C.}$ / 2 A Input: from 100 to 240 $V_{A.C.}$ / 0,3 A / 50 Hz
Status indicators	LEDs, for POWER, WiFi, LINE and NET (network), plus one LED per each LAN or WAN port.
Temp. range	Operating: 5^0 .... 50^0 C Storage: 0^0.... 60^0 C
Dimensions (L x W x H)	248 x 170 x 53 (mm) except protrusions
Weight	1100 g

7. OPERATING ENVIRONMENT

BYTTON HSDPA was designed for indoor use only, so you should NOT operate it outdoors.

You must install the BYTTON HSDPA equipment in closed rooms or enclosures, where the environment conditions should be:

- operating temperature range: from 5 to 50 degrees C
- relative humidity: from 10 to 85 %, non-condensing

You should avoid dust and prolonged exposure to sun radiation. In addition, BYTTON HSDPA must NOT be used in a flammable or explosive environment, or in locations where toxic or flammable gases may accumulate.

The equipment must be handled with care, to avoid mechanical shocks and blows.

BYTTON HSDPA should not be used in an environment with high level of EMI (electromagnetic interferences) that is in close proximity to high power equipment such as electric motors or heaters. In addition, it should not be placed near copiers, PC monitors, TV sets or other audio-video appliances.

In order to ensure adequate working temperature, the BYTTON HSDPA interface must not be used too near heat sources or in direct sunshine.

Also, it must not be overcrowded: you must leave free space around, below and above the BYTTON router. This is needed both for connecting phones / data / antennas cables, and also for ventilation (natural air cooling to dissipate the heat generated during operation).

Remember, when allowed operating temperature is exceeded this may not have an immediate, visible effect on the BYTTON unit, but it can result in unreliable operation, accelerated ageing and hence diminishing of lifetime.

When selecting the location for installing BYTTON HSDPA and its external antennas you must remember the recommendations described in the chapter about mounting the equipment.

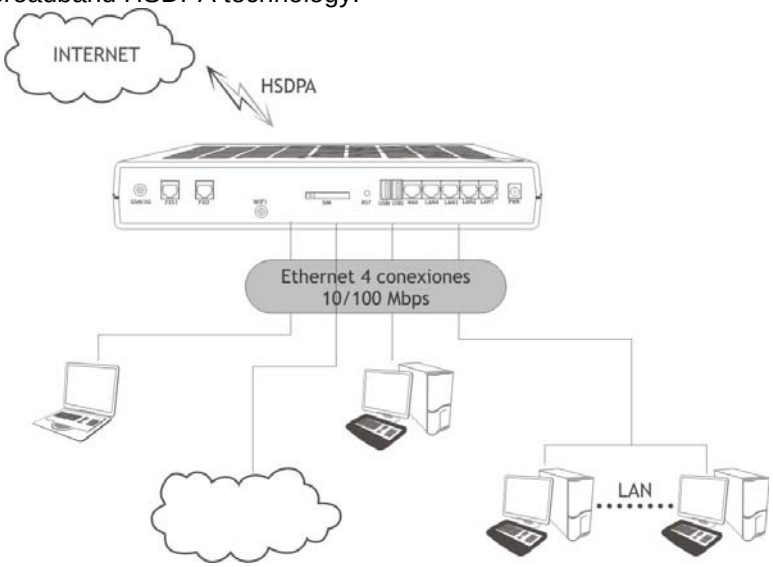
Topex BYTTON equipment does not include materials or components that are harmful to the environment.

When the life cycle of this equipment is finished and it cannot be repaired or re-used anymore, you should dispose of it in accordance with laws and legal regulations that are valid in your area.

8. APPLICATIONS

a) Wireless gateway/firewall/router using the HSDPA network

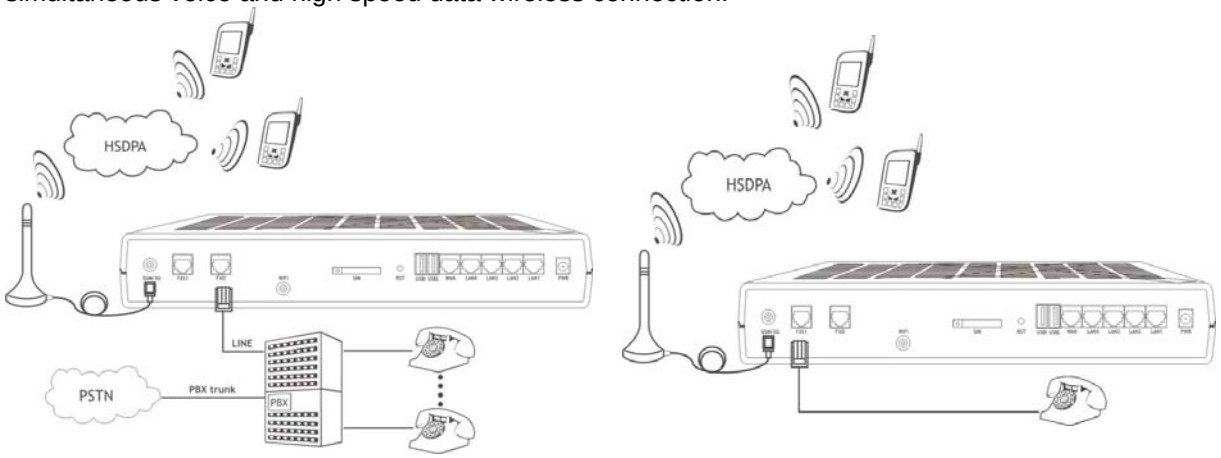
BYTTON was designed primary for wireless use, where it connects several computer, a local network or peripheral devices by means of its embedded HSDPA modem. BYTTON acts as a powerful residential gateway, being a compact, all in one box (NAT, PAT, router, firewall), connected to Internet via mobile broadband HSDPA technology.



You may connect to the BYTTON HSDPA equipment both wireless clients, via its embedded AP, and wired (Ethernet) clients, that is computers and various peripherals, at the same time.

The access to data traffic does no longer require additional investments on equipment or software (router, switch , software, wiring operations). BYTTON HSDPA allows connection to the local network (LAN) via four Fast Ethernet (10/100 Mbps) ports or via its AP.

These kinds of applications are especially suited for both home and small or medium business network environment, where land connections are not readily available. With BYTTON HSDPA, you get simultaneous voice and high speed data wireless connection.

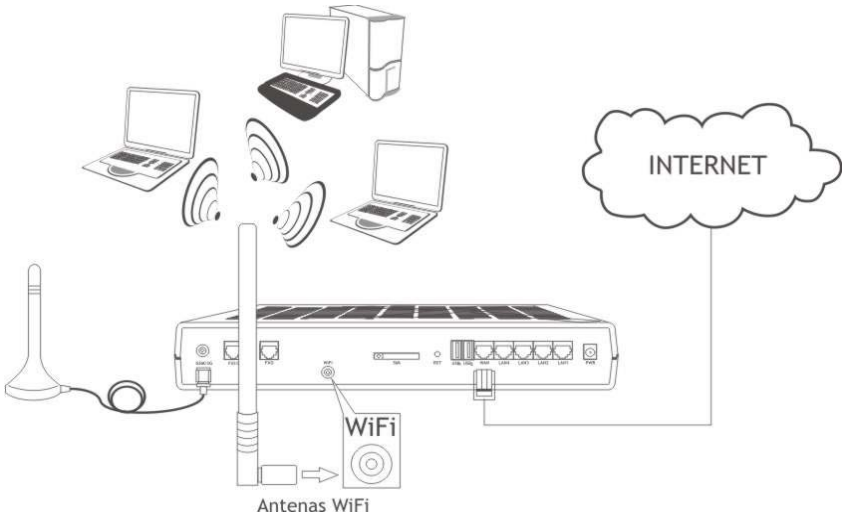


In addition, temporary events (festivals, sporting competitions, trade fairs and exhibitions) may benefit from the use of a wireless broadband router. Even if the temporary event is located in the heart of the city, getting a wired broadband connection for only 2-3 days makes no economic sense.

Fields of applications may include Advertising & Marketing, Property / Estate Agencies, Logistics, Recruitment, Travel & Hospitality, Healthcare, Media & Broadcasting , Insurance & Finance.

b) Broadband router with wireless local connections

You may use BYTTON without its mobile (HSDPA) module, connecting instead a cable or DSL or fiber modem to the WAN port of BYTTON. This way, the equipment acts a broadband router with wireless or wired local connection. Alternately, its failover feature allow Bytton to work **primarily** as router for the alternate connection, and when the wired Ethernet or PPPoE connection fails, it switches to using its embedded HSDPA modem:



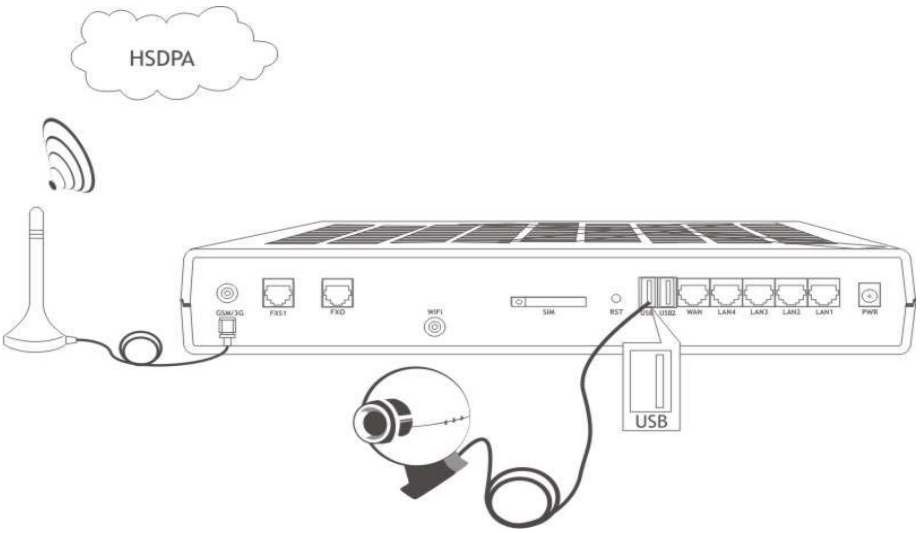
The embedded WiFi (802.11g) Access Point of Topex BYTTON allows immediate radio connection to computers or peripheral devices (such as notebooks, PDA, printers, IP phones, surveillance cameras or other devices equipped with WiFi interfaces).

You no longer need Ethernet cables to connect these devices and have all the advantages provided by the Wireless Access Points!

Still, the four LAN ports are available, and you may combine in different configurations the wired and wireless local connections.

In both home or small business environments BYTTON HSDPA allows flexible, mobile interconnection of desktop and notebook computers, printers and other peripherals such as scanners, playstations for on-line games, and provides web surfing, playing online games, netmeeting, video transmissions, listening to mp3 music, etc

c. Remote video surveillance with camera



With its built-in firmware, BYTTON HSDPA allows easy connection of one or several video surveillance cameras to a remote center, transmitting the still pictures or video stream via its embedded HSDPA modem.
The device can take over high-speed imaging inputs from different types of cameras (with USB, Ethernet or WiFi interfaces).

The USB webcams that are compatible with the PWC Linux driver may be connected **directly** to BYTTON, no additional firmware or software is required. The surveillance and the control of the camera may be performed remotely, from any web browser.

9. Glossary

3G – "Third generation" mobile networks, specially designed for high speed data services. The classic definition of wireless networks that following the 2G systems (GSM) and they offer high speed data services in addition to the basic voice capability. These 3G mobile communications systems provide an enhanced range of multimedia services (high speed Internet access, videostreaming, etc.). The high data transfer speed specific to the third generation communications network leads to an increased efficiency of information transmission, while the real time access to data and information means important savings of time and money. UMTS is the best known (but not the only one!) of the 3Gnetworks.
Access Point - The network hub device or "base station" for a wireless network. An access point (AP) is a device that allows wireless clients to connect to other wireless clients and it acts as a bridge between several local wireless clients and a another network, such as 3G mobile broadband network or wired Ethernet. BYTTON HSDPA acts as an AP and can be server to as many as 32 WiFi clients (notebooks, desktop PCs with wireless cards or USB adapters, PDAs, wireless peripherals and so on)
Broadband - A type of data transmission in which a single medium (radio, cable or fiber optics) carries several channels of data at once. Broadband is also associated with high transfer speed (at least 300 Kbps). HSDPA technology fully qualifies for mobile broadband connection!
CDMA – Acronym for Code Division Multiple Access. Advanced communications technology that is a driving force behind 3G wireless networks around the globe. CDMA ensures excellent quality of voice signal, without noise or interferences, high rate of data transmission and permits a uniform distribution of energy in the emitted bandwidth. UMTS makes use of the W-CDMA technology, wideband CDMA.
Client – wireless clients are the "mobile terminals" connected to your local WiFi network. These WiFi clients may be notebooks, desktop computers, PDAs, IP phones or other wireless devices.
CLIP - Acronym for **Calling Line Identity Presentation.** This feature allows the ID (phone number) of the caller to be displayed during the call. It is a service of the phone network. For end-users, this service is handy in order to screen incoming calls, prepare the specific response, greeting the caller by name or looking up for missed or unanswered phone calls. BYTTON HSDPA can use the CLIP facility to identify the subscribers who called and route the incoming calls according to their Caller ID.
CLIR - Acronym for Calling Line Identification **Restriction**. Feature that restrict the identification of your caller ID to the other party. This hides your identity from callers with Caller ID feature. You may activate this function on the Bytton equipment , thus disabling the sending out of Caller ID.
DISA – Acronym for **Direct Inward System Access.** This function allows an outside caller to directly access a local subscriber of the phone exchange by using DTMF codes.
The typical application is when you call directly a local subscriber without need for a human operator at the phone exchange. The BYTTON HSDPA equipment makes use of DISA-like routing to manage both incoming and outgoing calls without need for a human operator. For example a local subscriber may dial (using DTMF codes) a mobile number via the BYTTON HSDPA equipment.
DTMF - Acronym for **Dual Tone Multi Frequency,** also known as "touch tone". Advanced method for dialing a number, instead of the older Pulse mode. When you press a key on the keypad a combination of two audio frequencies is sent on the line. DTMF capability is important because it allows access to a wide range of interactive voice applications. The BYTTON equipment uses DTMF dialing to transmit the numbering from local subscribers to the mobile networks. Also, it uses dialing in DTMF mode to ensure phone connections without need for an operator at the PBX.
Device name - Also known as DHCP client ID or network name. Some ISP provide the customers with such device names, when using DHCP to assign addresses.
DHCP (Dynamic Host Configuration Protocol) - This protocol allows a computer (or many computers on your network) to be automatically assigned a single IP address from a DHCP server. DHCP is available on BYTTON HSDPA.
DNS – Acronym for Domain Name System (or Service), an Internet service that translates domain names into IP addresses. This allows the Internet hosts to use both addresses type domain name (such as topex.ro or linux.org), and addresses type IP numbers (for instance 192.17.3.4). The domain name addresses are intended for human users and are automatically converted into IP (numeric) addresses. Because domain names are alphabetic, they are much easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address.
DNS Server – computer able to answer to the interrogations in a DNS system. The DNS server maintains a database that includes the host computers with their domain names and the corresponding IP addresses. For instance, if you ask the DNS server for the domain name apex.com, it will return the IP address of the hypothetical company called Apex. DNS servers are linked in their network, so if one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is found. When a user enters a domain name into the Internet browser, the user is sent by the DNS Server to the proper IP address. The DNS server address used by the computers on your home network is the location of the DNS

DNS Server Address (Domain Name System) - DNS allows Internet host computers to have a domain name and one or more IP addresses. A DNS server keeps a database of host computers and their respective domain names and IP addresses, so that server your ISP has assigned.
Dynamic DNS - service that allows clients connecting to the Internet with a dynamic IP address to be able to use applications that require a static IP address. The Internet Service Provider changes the IP address of the users, but there are applications that work only with static (fixed) IP addresses. Dynamic DNS makes it possible for sites on the Internet to establish connections to you computer without need for tracking the IP address themselves. DDNS is useful both for wired or wireless (such as UMTS) dialup connection where at each connection a new address is assigned, and for DSL services where the address is changed occasionally by the ISP.
Domain Name Resolution - The resolving of a domain name. Internet applications don't communicate with domain names such as google.com or topex.ro, instead they use IP addresses (for example 193.226.61.95 or 216.239.39.99). Domain Name Resolution is the process (transparent for the user) of converting domain names into corresponding IP addresses. Every operating system has routines that deal with resolution of domain names.
Encryption - This provides wireless data transmissions with a level of security.
ESSID - Acronym for Extended Service Set ID. ESSID is one type of SSID (the other being BSSID). The ESSID is the identifying name of a wireless network. You can use a name that describes the network, such as „PurchasingnetworkA", „BYTTON_UMTS" or „InternetCafeDoris". This allows one wireless network to be clearly distinguishable from another. Also, this will ensure that only the users that have configured the same ESSID may access your WiFi network - you must have the same ESSID entered into the gateway and each of its wireless clients. You can also hide ESSID, to ensure that your Access Point is not visible to others. This increase the security – since the Wireless LAN network is invisible from outside, it will be more difficult for potential hackers to find out that there is a WiFi network available.
Ethernet - Standard for wired computer networks. Ethernet networks are connected by cables and hubs, and move data around. For wired connections, BYTTON HSDPA provides Ethernet 10/100 ports, four for the local LAN and one for WAN.
Firewall - System designed to prevent unauthorized access to or from a private network. The firewall determines which information passes in and out of and prevents anyone outside of your network from accessing your computer without authorization and possibly damaging or viewing your files. Any company with an intranet that allows its workers access to the wider Internet must use a software or hardware firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users have access to. Here the firewall is software a set of related programs (residing on the gateway server) that protect the resources of the local (internal) network.**FXS** - Acronym for Foreign Exchange Station. The FXS phone interface supplies ring, voltage, and dial tone for a "Station", that may be an analog phone, a modem, a fax machine, or any analog device of the final user. The FxS interface of the BYTTON HSDPA equipment may be used for connection either to an analog trunk of the PBX or directly to a standard fixed phone.
FXO - Acronym for Foreign Exchange Office. The Office phone interface connects to the public phone exchange (central office - CO), or a FxS board of the PBX. The FXO device gets power supply from the central battery and disk tone services. The FxO interface of the BYTTON equipment is used to connect the device to a local extension line (local subscriber) of the PBX. Both FxS and FxO interfaces use two wires.
Gateway - A network point that manages all the data traffic of your network, as well as to the Internet and connects one network to another. BYTTON is also gateway, since it interfaces between the local networks (wired or wireless) and the HSDPA mobile network or another broadband connection.
GRE – Acronym for Generic Routing Encapsulation. GRE is used as a tunneling protocol, which can encapsulate a wide variety of protocol packet types inside IP tunnels. IP tunneling using GRE protocol allows easy creation and expansion of a Virtual Private Network using the 3G mobile network. Topex BYTTON allows you to use two different GRE tunnels.
IP Address – Short from Internet Protocol address. The numerical address of a network device or resource as expressed in the format specified in the Internet Protocol (IP). In the current addressing format, IP version 4, the IP address is a 32-bit (4 bytes) sequence divided into four groups of decimal numbers separated by periods ("dots"). Each number can be zero to 255. These four groups of numbers look like "127.0.0.1" or „213.154.120.170". The four numbers in an IP address are used in different ways to identify a particular network and a host on that network.
IP – Acronym for Internet Protocol. It is the protocol from TCP/IP that directs the way data is sent from one computer to another on the Internet. The messages are divided into data packets, routed from the sender network to the receiver network and there re-assembled in the right order to re-create the original message. Because a message is divided into a number of packets, each packet can, if necessary, be sent by a different route across the Internet. These data packets can arrive in a different order than the order they were sent in. The Internet Protocol just delivers them. It's up to TCP protocol (Transmission Control Protocol) to put the packets back in the right order.

Note that IP is a connectionless protocol, which means that there is no continuing connection between the end points that are communicating. IP corresponds to the layer 3, the Networking Layer from the Open Systems Interconnection (OSI) communication model.

IP PnP – Acronym for IP Plug-n-Play, capability that allows instant Internet access for the users, no matter what their network settings are. With IP PnP the subscribers may connect with ease for broadband access without having to re-configure any of their device IP settings including DHCP, DNS, Proxy and dynamic and static IP address assignments. The Topex device automatically identifies users' network settings: static or dynamic IP, gateway, proxy, etc. so the users no longer need to re-configure their PCs', notebooks or PDAs' when they connect to the Topex equipment. With its IP Plug and Play technology, BYTTON ISDN accepts any client configuration for log-on, the end-users can leave unmodified their default network, e-mail, or browser settings. This technology used by BYTTON is also called PnP Connectivity Service or Internet Access with "Zero Configuration" .

IP Tunneling - a tunneling protocol encapsulates a packet of the same or lower protocol, while in a regular protocol, the lower layer protocol encapsulates the higher level protocol. In order to achieve a Virtual Private Network (corporate network) you must ensure the port forwarding (tunneling), that is the transmission of private data through a public network such as 3G. The routing nodes in the respective public network must not be aware that the transmission is part of a private network. Tunneling means the encapsulation of the data and protocol information of the private network within the transmission units of the public network. Widely used tunneling methods are the Point-to-Point Tunneling Protocol (PPTP) developed by Microsoft and generic routing encapsulation (GRE), developed by Cisco Systems. BYTTON ISDN equipment supports GRE protocol.

ISP (Internet Service Provider) - An ISP is a business that allows individuals or businesses to connect to the Internet. Users log on to the Internet using an account with an ISP or Internet Service Provider. ISPs can serve IP addresses dynamically, or assign static (fixed) IP addresses to individual computers. In this case, the Internet provider is the operator of the 3G mobile network.

LAN - Acronym for local area network (computer network that spans a relatively small area). A group of computers, workstations and associated devices that share a common communications line or wireless link and are located in a relatively limited area, typically inside the same office building. The communications link that interconnects these computers allows any device of the network to interact with any other from the same network. The devices that compose a local network (workstations, personal computers and peripherals) are called nodes and typically share the resources of a single processor or server. This server has resources (applications, processing and data storage capabilities) that are shared in common by multiple computer users. The LAN can be connected to other local networks over any distance via phone lines, wireless links or other connections, and the system of LANs connected in this way is called a wide-area network (WAN).

The LAN may also be connected to the Internet through a gateway. BYTTON ISDN equipment performs as a gateway since it interfaces between a local Ethernet or WiFi network and the CDMA wireless data network.

MAC Address (Media Access Control) - A MAC address is the hardware (physical) address of a device connected to a network.

All network interface controllers must have a hard-coded and unique MAC address. The MAC address is applied at the factory and uniquely identifies network hardware, such as a Ethernet cards, modems or wireless adaptors on a LAN or WAN. The first part of the address is unique to the company that produced the device, and beyond that it is a sequence of digits unique to a single device manufactured by a company.

MTU - Acronym for Maximum Transmission Unit. Generally, the size of the largest datagram that can be passed by a layer of a communications protocol (that can be transmitted or received through a logical interface). All messages larger than the MTU will be divided into smaller packets before being sent. In our case MTU is the largest physical packet size, measured in bytes that a network can transmit. The size includes the IP header but does not include the size of any Link Layer headers or framing.

Different networks have different values for MTU, which is set by the network administrator. Most networking technologies have a default MTU size: this is 576 for many PPP connections, 1500 for Ethernet networks, 65K for HYPER channel, etc.

NAT - Network Address Translation. NAT is an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and another set of addresses for external traffic. On the gateway, NAT software performs all necessary translations of the IP addresses. There are several purposes for NAT usage:

Provides a type of natural firewall by hiding all the internal IP addresses from the Internet. Only the single IP assigned to the router is visible from the Internet.

Several computers on the local network to use one IP address, enabling access to the Internet from any computer network without the need to get more IP addresses from the ISP

local computers are not directly reachable from the Internet, making them more secure

the company can use several internal IP addresses. Since they're used only internally, there is no

possibility of conflict with IP addresses used by other companies or organizations.
NTP - Acronym for **N**etwork **T**ime **P**rotocol. Internet standard protocol used to update the real-time clock in a computer. It assures accurate synchronization to the millisecond of computer clock times in a network of computers.NTP is very useful in packet-switched, variable-latency data networks. In case of BYTTON, if you want to measure the performances of the network, you need accurate, universal time-stamps for the data packets.
NTP runs as a continuous background client program on a computer and it sends periodic time requests to servers, obtaining server time stamps and using them to adjust the client's clock. NTP uses UDP port 123 as its transport layer. It is designed particularly to resist the effects of variable latency. There are numerous primary and secondary servers in the Internet that are synchronized to the Coordinated Universal Time (UTC) via radio, satellite or modem. For more information, visit www.ntp.org.
PBX - Acronym for Private Branch eXchange. The PBX is a small, enterprise version of the larger central switching office of the phone company. A PBX is a **private** telephone switch. It is connected to groups of trunks (junctions) from one or more central offices and to all of the telephones at the location (subscribers, local extensions) served by the PBX. Current exchanges are in fact PABX, automated PBX, which don't require a human operator to route the calls. The BYTTON HSDPA equipment was designed to work together with a PABX with analog trunks to route the calls. Bytton may be connected to the PBX either on a trunk line or on a subscriber line (local extension).
PSTN - Acronym for **Public Switched Telephone Network (s)**.
This is the classic international fixed telephony system based on copper wires that carry voice and data. Analog (mostly) or digital technology is used to provide voice grade services for the users that access that network via an **analog** interface. The BYTTON device connects to a PBX that has trunks going to the PSTN, so the equipment performs as an interface between the mobile network (GSM/GPRS/EDGE/UMTS) and the PSTN.
PPP - Acronym for Point-to-Point Protocol. Network protocol widely used to connect computers to the Internet. Works on the data link layer of the OSI model. PPP sends the TCP/IP packets of the gateway to a server that puts them onto the Internet. It is more stable than the older SLIP protocol and provides error-checking features.
PPP is the Internet standard for dial-up modem connections, no matter if they are phone line modems of high-speed UMTS wireless devices such as the embedded HSDPA modem of BYTTON.
PPPoE - Acronym for Point-to-Point Protocol over Ethernet. A method of secure data transmission, PPPoE using Ethernet to connect to an ISP. The PPP traffic is sent over Ethernet to the Internet through a common broadband medium. The users have the appearance of "dialing" the Internet, but their computers are in fact always connected.
PPPoE supports a broad range of existing applications and services, from authentication, accounting and secure access to configuration management. BYTTON supports on the WAN side either PPP or PPPoE connection.
Radio Channel - Wireless access points allows you to choose different radio channels in the wireless spectrum. A wireless LAN device operates within the 2.1 GHz spectrum and a channel is within a FCC specified range, similar to any radio channel. The Access Point of BYTTON can select the radio channel automatically, or you can specify a certain channel, if you want to.
RIP - Acronym for Routing Information Protocol. RIP for IP is a distance-vector routing protocol, which is the main dynamic routing protocol used in small or medium-sized IP internetworks. For dynamic routing, BYTTON HSDPA supports protocols RIP v2 and OSPF.
Routing -The process of determining and prescribing the path or method to be used for establishing connections and forwarding data packets. In a network, a 'routing switch' is a device that combines the functions of a switch, which forwards data by looking at a physical device address, and a router, which forwards packets by locating a next hop address. Each host with a router in the network uses the routing table information to determine the next host to route a packet to for a specified destination.
BYTTON performs as a router for the wired or wireless local network where it is connected. It can perform both static routing (with fixed, pre-defined routes) and dynamic routing. Dynamic routing is more complex than static routing, but it provides several benefits. It ensures scalability and adaptability. The routes are dynamic, interactive, permanently updated. Routers learn about the network topology by communicating with other routers so it may select a better route, optimized for each time period. The BYTTON equipment supports different protocols for dynamic routing, such as RIP v 2 for distance vector routing and OSPF for link state routing.
S-HTTP - Acronym for SECURE HYPERTEXT TRANSFER PROTOCOL. A secure way of transferring information over the Web, by using an application-level encryption scheme. S-HTTP is an extension of the normal HTTP with security enhancements for WWW-based commerce. Web pages that use S-HTTP have a URL starting with https://. Typically HTTP data is sent over TCP/IP port 80, but HTTPS data is sent over port 443. The standard was developed for secure transactions, and uses 40-bit encryption ("weak" encryption) or 128-bit ("strong" encryption). The HTTPS standard supports certificates and allows encryption, digital signatures, authentication, or any combination of these. The S-HTTP type of

transaction security is more secure than a user ID and password, thus it is mostly used by financial institutions (for example for credit-card purchases over the Web). Since BYTTON provides ensures S-HTTP, this means a higher degree of security for you.

SMS - Acronym for **Short Message Service**; means the transmission of short text messages to and from cellular phones. The messages must be text only (no images or graphics) and not longer than 160 alpha-numeric characters. Operators of Mobile Phone Networks use a spare data channel to send SMS messages. You may send SMS messages to another mobile subscriber, the mobile operator can send you phone settings over-the-air or commercial companies may send dedicated content to your mobile terminal. The embedded firmware allows BYTTON equipment to send and receive SMS (via mobile network) from the computer connected to it.

Static packet filter - One of the simplest and least expensive forms of firewall protection is known as static packet filtering. With static packet filtering, each packet entering or leaving the network is checked and either passed or rejected depending on a set of user-defined rules. Dealing with each individual packet, the firewall applies its rule set to determine which packet to allow or disallow. The static packet filtering firewall examines each packet based on the following criteria:

* Source IP address
* Destination IP address
* TCP/UDP source port
* TCP/UDP destination port

Static packet filtering is easy to implement and configure and does not use a lot of resources, but its efficiency is limited. Basic packet filtering firewalls are susceptible to IP spoofing, where an intruder tries to gain unauthorized access to computers by sending messages to a computer with an IP address indicating that the message is coming from a trusted host. Another shortcoming is that this form of firewall rarely provides sufficient logging or reporting capabilities.

SPI - Acronym for Stateful packet inspection. The embedded BYTTON firewall also performs stateful packet inspection. This approach examines the contents of packets rather than just filtering them. It takes into account not only the addresses of the data packets but also the contents and the state of the connection. Stateful means they take into account the state of the connections they handle so that, for example, a legitimate incoming packet can be matched with the outbound request for that packet and allowed in. In addition, an incoming packet masquerading as a response can be blocked if the firewall knows that the outbound request is in fact nonexistent. Rather than controlling the individual data packets. SPI uses smart rules, thus enhancing the filtering process and controlling the network session. Static packet filtering cannot stop DOS attacks But SPI closes ports until legitimate users request them opened so it prevents certain kinds of Denial of Service attacks. Since SPI firewalls compare packets to previous packets, the packets that violate the rules can be dropped.

SSID - Service set identifier, the name of a wireless local area network (WLAN). A code attached to all data packets on a wireless network for identification purposes. Besides identifying each packet, SSID serves also to identify a group of wireless network devices used in a given "Service Set". This ID allows multiple wireless Ethernet networks to be active at the same time in the same location. You may allow or disable the "public SSID", which is set on the access point and broadcast to all wireless devices in range. If you disable the automatic broadcasting of SSID feature the security of the network is increased, people who don't know this ID cannot connect to the WiFi LAN.

TCP/IP – Acronym for Transmission Control Protocol / Internet Protocol. It was established by the Defense Department of the USA for communications between computers. It has been at first incorporated in Unix operating system but has become the de facto standard for data transmission via networks, including for Internet.

Currently TCP/IP is the basic communication language or protocol of the Internet, but it can also be used as a communications protocol in private network. TCP/IP uses the client/server model of communication in which a computer user (a client) requests and is provided a service (such as sending a Web page) by another computer (a server) in the network. TCP/IP is a two-layer program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination. For details see the definitions of those protocols that Access -LAN supports.

TCP – Acronym for Transmission Control Protocol. In TCP/IP, the TCP part is the one that takes care of keeping track of the individual units of data (packets) that a message was divided into for efficient routing through the Internet. TCP is known as a connection-oriented protocol, which means that a connection is established and maintained until the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.

At the destination, TCP reassembles the individual packets and waits until they have all arrived to forward them to you as a single file. It also checks the received packets. TCP acts at the transport level

(level 4) of the ISO/OSI model. See also ISO/OSI model, packet, TCP/IP.
UDP – Acronym for User Datagram Protocol. It is a simpler protocol than TCP/IP that corresponds to the transport layer of the ISO/OSI model. UDP converts the messages generated by the application into data packets to be sent through IP, but does not check if the messages have been transmitted correctly or not.
UDP allows individual packets to be dropped (with no retries) and UDP packets to be received in a different order than they were sent. Consequently UDP is more efficient but less reliable than TCP and is used to different purposes - primarily for broadcasting messages over a network. With UDP, reliability is wholly in charge of the application that generates the message.
UDP is used often in applications such as videoconferencing or games where optimal performance is preferred over guaranteed message delivery.
WiFi - Acronym for Wireless Fidelity. High-speed wireless access technology that allows users to connect to the Internet without using any form of wiring or cable. The service is available to anyone with a desktop computer, notebook or personal digital assistant (PDA) equipped with 802.11 wireless access capability. The embedded Access Point of BYTTON ISDN supports both standard 802.11b and 802.11g.
WAN - Acronym for Wide Area Network. A system of LANs, connected together. A
Wan is a network that connects computers located in separate areas, (i.e., different
buildings, cities, countries). The Internet is a wide area network. BYYTON features a WAN port, allowing connection to another network or alternate broadband service provider.
WLAN - Acronym for Wireless Local Area Network. A group of PC computers, notebooks, PDAs', peripherals and other devices connected wirelessly in a small area.
WEP - Acronym for Wired Equivalent Privacy, encryption protocol for WiFi networks. As its name says, WEP was designed to provide for WLAN a level of privacy equivalent to that of an unsecured wired LAN. WEP is used at the two lowest layers, the data link and physical layer. To read a WEP encryption on file you need a secret key or password to decrypt it. There are two main types of WEP encryption, symmetric and respectively asymmetric WEP (public key WEP encryption). and WEP encryption. WEP encryption standard employs 40-bit encryption and a 128-bit WEP encryption option. Remember that only when using the 128-bit keys WEP encryption it ensures the same level of security as the unencrypted wired Ethernet. WEP is NOT an industrial strength security algorithm. It is vulnerable because of relatively short IVs and keys that remain static.

The manufacturer reserves the right to modify the product and manual for the purpose of technical improvement without prior notice. The manufacturer guarantees the good functioning of the product provided that it has been correctly installed and the directives for storage and usage have been respected. The warranty implies exclusively repairing or replacing the defective unit. The warranty does not include any indirect losses or loss of profit. The manufacturer is not liable for any damage, whether direct, indirect, special, incidental, or consequential, as a result of using Topex BYTTON HSDPA.

No part of this manual may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written permission of the company TOPEX S.A.

It is certified hereby that the Topex BYTTON HSDPA unit is manufactured in concordance with the legal provisions concerning responsibility towards the quality of delivered products, fulfills the quality parameters specified in its "User's manual" and is fit for the purpose for which it has been designed. It also warrants that the equipment will perform substantially in accordance with the accompanying documentation.

Any comments, suggestions and proposals of yours concerning our products are welcome and we are gladly waiting for your feedback:

TOPEX S.A.
Feleacu street, no. 10, sector 1
Bucharest 014186 ROMANIA
Tel: +4021 408.39.00
Fax: +4021 408.39.09
E-mail: topex@ topex.ro
Web: http://www.topex.ro